NEUMANN JÁNOS SZÁMÍTÓGÉPTUDOMÁNYI TÁRSASÁG

MŰSZAKI ÉS TERMÉSZETTUDOMÁNYI EGYESÜLETEK SZÖVETSÉGI TAGJA

KÖZLEMÉNYEI 2.

ADATVÉDELEM '82

PÉCS, 1982 NJSZT

A NEUMANN JÁNOS SZÁMITÓGÉPTUDOMÁNYI TÁRSASÁG

Baranya megyei szervezete és Számitóközpont vezetési Szakosztálya keretében müködő Számitástechnikai Jogi Munkabizottság rendezésében lezajlott

ADATVÉDELEM '82

Konferencián

elhangzott előadások

Pécs, 1982. október 25-27.

Szerkesztette: Weisz Istvánné dr.

Készült: A Pécsi Tempó Ált.Szolg.Szövetkezet
Sokszorosító-Könyvkötő Üzemében - 1983. évben, -
A/4 form.5oo pld.MSz.132.
Fel.vez.: Negele Tibor.

ISBN 963 - 8431 - 32 - 6

TARTALOMJEGYZÉK Oldal

AZ ADATVÉDELEM KÖRNYEZETE, ELVI MEGALAPOZÁSA, KAPCSOLÓDÓ PROBLÉMÁI

AZ ADATVÉDELEM MÜSZAKI-TECHNIKAI VONATKOZÁSAI

AZ ADATVÉDELEM PROGRAMOZÁS- ÉS ÜZEMELTETÉSTECHNOLÓGIAI KÉRDÉSEI

AZ ADATVÉDELEM KÖRNYEZETE, ELVI MEGALAPOZÁSA, KAPCSOLÓDÓ PROBLÉMÁI

dr. Varga Lajos:

A SZÁMITÁSTECHNIKA ALKALMAZÁS NÉHÁNY IDŐSZERÜ KÉRDÉSE +

A számitástechnika elterjedésének nemzetközi tendenciái

- A számitástechnika növekvő fejlődése, az információtechnika kialakulása. A számitógépek számának növekedése.
- A mikroelektronika szerepe. A nyugat-európai fejlődés főbb tényei. Az állami szervezetek, a nagy vállalatok, a kisvállalatok, az oktatás és a háztartások részesedése, nyugat-európai számitógépállomány szerkezetének átalakulása.
- Ausztria példájának vizsgálata, a számitógéppark növekedési üteme /nyolc év alatt négyszeresére nőtt/, a folyamatirányitó és miniszámitógépek /19., ill. 4-szeres növekedés/, a ráforditások részesedése a BNT-ből, az iparirányitási és irodai alkalmazások terjedése, a terminálok számának változása, a távadatfeldolgozás előnyei.

A számitástechnika alkalmazás tervezése

A központi fejlesztési programok, az SZKFP, a VI. ötéves tervi konkrét program. Progressziv iparág - alkalmazási kör a teljes népgazdaság.
Információ sajátos érték, gazdálkodni kell. Nő az adatvédelem, adatbiztonság szerepe.
A tervidőszak jellegzetességei: alkalmazás orientáció.

- az alkalmazás jelentősége az egyes területeken;
- nő az információ értéke és a biztonság jelentősége;
- adatkapcsolatok - adatbázisok - kiterjedtség - személyi adatok - hálózati adatkezelés -

---

+ A konferencián elhangzott részletes megnyitó előadás tematika-vázlata.

- technikai megoldás és a biztonság összefüggései, TAF; adatsérülékenység.

Hatékonyság és adatbiztonság

Nem naturális, nem eszközkihasználás; megfelelő módon és szinten álljanak rendelkezésre.
Biztonsági feltételek, hatékonyságromlás, költségnövekedés.
Hatékonyság és összehangolás összefüggései: az államigazgatási alkalmazásokban; államigazgatási információrendszerek komplex összehangolása, szervezetek közötti összehangolás, államigazgatás és lakossági kapcsolatok. Hatékonyság vizsgálat a gazdálkodó szervezeteknél.
A szolgáltató szervezetek szerepe a hatékonyság biztositásában. Hatékonyság elemzés az információ életciklusának elemeiben.

Számitástechnikai erőforrások és az adatbiztonság

1. Eszközök: ESZR - MSZR forrásból. Megbizhatóság, müszaki-technológiai szinvonal, folyamatos alkatrészellátás, szoftver ellátás /eszközkompenzáló-hatás/. Embargó korlátok.
Az eszközállomány változása: bruttó érték, volumen, korösszetétel és a korszerü feldolgozási technológiák. Eszköz árszinvonal hátrányos következményei az alkalmazásra. Eszközkihasználás.

2. Szoftverellátás: kedvező változások; egységes ESZR/MSZR alapszoftver elemek forgalmazása; szolgáltatások javulása; általános programtermékek beszerzése /TAF vezérlő, interaktiv program fejlesztő rendszerek stb./; tipus program fejlesztések; szocialista eredetü programtermékek; a SZAFA az általános programrendszerek forgalmazásában. Szoftver ellátás és adatbiztonság növekedés.

3. Szolgáltatások: 76 szolgáltató, 1900 igénybevevő fogyasztó szervezet; szoftver szolgáltatások növekvő részaránya; szolgáltatások csökkenő dijszintje; számitástechnikai szolgáltató szervezetek szerepe.

4. Kutatás - fejlesztés /erőforrás - adatbiztonsági tartalék/. Mintarendszerek, technológia, TAF, mikroszámitástechnika, hosszutávu koncepció.

Gazdasági-jogi szabályozás - adatbiztonság

Az alkalmazás gazdasági jogi környezete. Informatikai termelés. Normativ gazdasági eszközök. Normativ szabályozás: fogalmi rendszer, ágazati osztályozás, alkalmazási termékek és szolgáltatások, ITJ felülvizsgálat. Árrendszer. MÜFA lehetőségek.

Nemzetközi kapcsolatok - adatbiztonság

Szocialista alkalmazási, ipari együttmüködés. Alkalmazások terjedése. Együttmüködés és adatbiztonság. Információ rendszerek közötti kapcsolatok.
Adatbiztonság tulnő a határokon. Nagy információ rendszerek - információ tartalom, adatbiztonság.
Adatkommunikáció. Telematika. Információszolgáltatás. Szakositott adatbankok /500/ 70 millió tétel, olcsó használat.

A hazai adatvédelem helyzete, fejlődése

Jogi szabályozás, több lépcsős. Titok, vagyon és tüzvédelem, Irányelvek, módszertani segédanyag. Bonyolult struktura. Személyhez füződő jogok, szolgálati titok.
Tárcautasitások - SZVSZ-ek. Az alkalmazás gondjai. Adatvédelmi felelősök oktatása, képzése. Tananyag készités. Szakmai specializálódás.

A hazai adatvédelmi szabályozás nemzetközi összehasonlítása. Egyezőség és különbségek a személyiségi jogok védelmében. A polgári demokrácia és a szocialista demokrácia elvárásai. Tartalmi és formális elemek. A személyhez fűződő jogok védelme: Statisztikai Törvény; Népességnyilvántartási törvény; levéltári tvr.; személyzeti kormányhatározatok. Alkotmányunk VII. fejezete. Ptk a személyhez fűződő jogokról. Technikai fejlődés, személyiségi jogok kiteljesedése, fejlődési követelmények.

Dr. Törő Károly:

A SZÁMITÁSTECHNIKAI ADATVÉDELEM ÉS A SZEMÉLYISÉG-VÉDELEM

A személyiség

Az utóbbi évtizedekben a személyiség kérdései a társadalmi és a tudományos érdeklődés előterébe kerültek. A személyiség sokfajta - többek között filozófiai, pszichológiai, szociológiai és jogi - vizsgálódás tárgya.

A személyiség bonyolult, összetett és ellentmondásos jellegü emberi valóság. Elválaszthatatlan a közösségtől, csak a közsség utján és által érvényesülhet, de viszonylag el is különül a közösségtől, ez az elkülönülés adja a személyiség sajátos, egyéni jellegét. A személyiség alapja az ember testi- anyagi felépitése, a személyiség mégsem azonos az ember biológiai létével, nem az ember keze, feje, idegrendszere önmagában, nem csupán természeti, hanem az erre épülő társadalmi valóság. Az ember belső valóság, sajátos emberi minőség, amely környezetében, a társadalomban nyilvánul meg. Megvalósulásának a feltétele, hogy a társadalom önálló és egyenrangu tagjának ismerje el az embert. Ez a társadalmi elismerés sajátos értékjelleggel ruházza fel emberi mivoltunket. Mindez hosszu történelmi folyamat, amely lényegében még napjainkban sem fejeződött be. A régebbi társadalmi rendszerekben a személyiség, mint a vagyoni viszonyoktól elkülönült önálló érték ismeretlen volt. Olyan társadalmi rendszerek is voltak, amelyekben az emberek egy részét - a rabszolgákat - dolgok módjára értékelték, vagyontárgynak tekintették. Mai társadalmi rendszerünk a személyiség rangjával ruház fel minden embert.

A személyiség az emberi egyed társadalmi minőségét, társadalmi értékjellegét fejezi ki. Alapja az a társadalmi szükséglet, amelyet kielégiteni hivatott, nevezetesen az ember mint személy önmegvalósitása, részvétele a társadalomban. A személyiség rendkivül sokrétü, összetett, mégis egységes jelenség. Számos olyan eleme van, amely önmagában is alkalmas valamely eszmei szükséglet kielégitésére, pl. az ember hire, neve, képmása, személyes titka stb. Mindez azonban elválaszthatatlan az egyetlen és egységes személyiségtől.

A személyiség jogi védelme

A jog célja a társadalmi szükséglet-kielégités szolgálata, elősegitése. Ezért a jognak a személyiség érvényesitését, az emberi egyed önmegvalósitását, a társadalomba való részvételét is szolgálnia kell. A jogi védelem különböző formában és módon valósul meg. Kiemelkedő személyiségi jogosultságainkat az Alkotmány alapjogként határozza meg. Nemzetközi jogi jellegü védelem érvényesül az ugynevezett emberi jogok tekintetében. A büntetőjog sajátos büntetőjogi szankciók alkalmazását teszi lehetővé egyes társadalomveszélyes személyiségi jogokat sértő cselekmények esetén. Bizonyos foku személyiségvédelmi szerepet töltenek be az államigazgatási jog, a családjog, ill. a munkajog rendelkezései is.
A legátfogóbb, legszélesebb körü személyiségvédelmet a polgári jog biztositja. A polgári jog a személyiség bármiféle megnyilvánulását védi az illetéktelen beavatkozástól. Egyrészt általános körü védelmet nyujt a személyiséget bármi módon jogellenesen sértő cselekményekkel szemben. Másrészt külön is védi a személyiség egyes legfontosabb megnyilvánulásait: igy az ember életét, egészségét, testi épségét, a személyes szabadságot és a lelkiismereti szabadságot, az ember hirnevét, becsületét, emberi méltóságát, nevét, hangját, kép-

mását, a személyes titkot, a szellemi alkotást és a kegyeletet.

A személyiségvédelem és a számitástechnika

A jog rendeltetése a társadalmi fejlődés szolgálata, ezért a jog célkitüzéseit és érvényesülését mindig a társadalmi fejlődés igényei határozzák meg.

Korunk társadalmi fejlődésének fontos összetevő eleme az un. tudományos-technikai forradalom, amely sajátos módon befolyásolja a személyiségvédelmet is. A müszaki fejlődés az ember anyagi életszükségleteinek egyre tökéletesebb kielégitését segiti elő. Ezáltal - megfelelő társadalmi feltételek esetében - közvetetten a személyiség megvalósitását is szolgálja. A fejlődésnek azonban vannak hátrányos kisérő jelenségei, ezek kiküszöbölésére is törkedni kell.

A müszaki tudományos-technikai fejlődés körében nagy jelentősége van a számitástechnika fejlődésének. Ez a fejlődés a társadalmat, és a társadalmon keresztül az egyes embert is szolgálja. Közvetetten elősegiti az ember önmegvalósitását, személyiségének az érvényesitését. Ezen a területen is tapasztalhatók viszont bizonyos negativumok, bizonyos veszélyek.

A személyiség fontos jellegzetessége a viszonylagos elkülönülés: minden ember önálló egyedként vesz részt a társadalom életében. A társadalom tagját nem lehet azonositani pl. a gépalkatrésszel, mert nem csupán része a társadalomnak, hanem körülhatárolt, viszonylagosan zárt külön világ.

A személyhez hozzátartozó adatokat tartalmazó széleskörü szá-

mitógépes nyilvántartások ennek a különállásnak a fellazitásával fenyegethetnek, nyilvántartási számként kezelhetik az embert, mint leltári tárgyat, elméleti jellegüvé változtathatják a személyes titokhoz való jogot. Az ember személyes körülményeinek a nyilvántartására vonatkozó személyiségkorlátozó jelleget a számitógépes nyilvántartásoknál sokkal kevéssé hatékony nyilvántartások idejében is észlelte a költő, aki igy kesergett: "Beirtak engem mindenféle könyvbe, és minden módon számon tartanak, ó megalázó, hogy rab vagyok és nem vagyok szabad. Nem az enyém már a kezem, a lábam, és a fejem: az is csak egy adat." /Kosztolányi Dezső: A bus férfi panaszai/ Mindez fokozottan érvényes a korábbi nyilvántartásoknál sokkal szélesebbkörü számitógépes nyilvántartásra.

A számitógépes nyilvántartás veszélye az is, hogy adatait fel lehet használni az eredeti rendeltetésétől eltérő célra is.

Mindez természetesen nem jelentheti azt, hogy a müszaki fejlődés veszélyezteti az egyén személyiségi értékeit. A gép nem lehet felelős a személyiség magán-autonómiájának a válságáért. A müszaki eszközökkel vissza lehet élni, az eszközök hatékonyságának a fokozódásával fokozódik a visszaélés lehetősége is. Ez azonban nem jelentheti azt, hogy számüzni kellene a hatékonyabb müszaki eszközöket. A gépet az ember alkalmazza, soha nem a gép, nem a müszaki eszköz, csupán az ezt felhasználó emberi magatartás veszélyezteti az emberi személyiség önállóságának a határait. Ennek a megelőzése érdekében korszerü és hatékony személyiségvédelemre van szükség. A müszaki eszközök fejlődésével lépést kell tartania a személyiségvédelmi eszközök fejlődésének is.

Mindez a számitástechnikai eszközökre is vonatkozik. Ezen a területen is ki kell épiteni a korszerü személyiségvédelemre

alkalmas biztositékok rendszerét.

A számitógépes nyilvántartással kapcsolatos személyiségvédelem legfontosabb biztositékai: a nyilvántartott adatok valódiságának és az ezzel kapcsolatos személyes titoknak a megőrzésére vonatkozó intézkedések.

A nyilvántartott adatok valódiságának a védelme

Polgári jogunk személyhez füződő jogként védi a hirnevet. A Ptk 78. §-ának a rendelkezése szerint a jóhirnév sérelmét jelenti a valótlan vagy a valóság hamis szinben történő feltüntetésére alkalmas tényállitás, adatközlés, hiresztelés. A birósági gyakorlat szerint hiresztelésnek kell tekinteni a más tól szerzett valótlan adatok egyszeri továbbadását is.

Számitógépes nyilvántartásnál a jogsérelmet meg kell állapitani már akkor is, amikor a valótlan /valóságot hamis szinben feltüntető/ adat a nyilvántartás részévé válik.

Mindenkinek fontos személyhez füződő érdeke, hogy a személyisége t a valóságnak megfelelő módon ismerjék és értékeljék. A személyre vonatkozó a valósággal ellentétes adatok gátolják a személyiség valósághü értékelését. Ezért az, akinek a személyét érintő adatait nyilvántartják, megkövetelheti, hogy ezek az adatok mgfeleljenek a valóságnak. Ez a követelmény bármiféle nyilvántartásra vonatkozik, de a számitógépes nyilvántartások tekintetében ezt a kérdést - különös jelentőségükre tekintettel - a törvény külön is szabályozza.

A Ptk 83. §-ának a /3/ bekezdése értelmében, ha a nyilvántartásban szereplő valamely tény vagy adat nem felel meg a valóságnak, az érintett személy ennek a helyesbitését birósági uton is kérheti. Külön jogszabályi rendelkezés esetében

lehetőség van arra, hogy a birósági eljárást államigazgatási eljárás előzze meg. Ilyen rendelkezés hiányában a fél közvetlenül fordulhat a bírósághoz. A bíróság a bizonyitási eljárás alapján állapitja meg a valóságos tényeket, illetve adatokat, és kijavitásra kötelezheti a számitógépes nyilvántartást kezelő szervet.

E jog gyakorlásának az előfeltétele, hogy az érintett személy ismerje a róla nyilvántartott adatokat. Ezért irja elő a jogszabály, hogy csak akkor lehet megtagadni az érintett személy tájékoztatását ezekről az adatokról, ha a tájékoztatás állami vagy közbiztonsági érdeket sértene. Ezt a rendelkezést megszoritóan kell értelmezni. A saját személyére vonatkozó adatokat, tényeket, mindenki saját maga ismeri a legjobban, ezek az adatok elsősorban rá tartoznak. Ezért általánosságban nem lehet megállapitani azt, hogy valakinek a saját személyét érintő adatok nyilvántartásának a megismerése az állam vagy a közbiztonság érdekeit sérti. Ez legfeljebb más adatokkal és tényekkel való összefüggésben lenne megállapitható. Ilyenkor azonban lehetővé kell tenni, hogy az érintett személy a többi adatoktól elkülönitetten ismerje meg a saját személyére vonatkozó nyilvántartott adatokat.

A személyes titok védelme

Minden ember jogosult a személyes természetü, személyére vonatkozó, személyiségét érintő adatokat, tényeket, ismereteket megőrizni, az érintett személy rendelkezésétől függ, hogy ezeket mikor, milyen módon és terjedelemben hozza mások tudomására. Lényegében ezt hivatott biztositani a személyes titok védelme, mint a személyiségvédelem egyik fontos területe.

A személyes titok a személyiség elkülönülési mozzanatát fejezi ki a társadalomhoz tartozás és a társadalom tagjaitól való viszonylagos elkülönülés szerves egységének a keretében. A személy éppen ezáltal lehet önálló és egyenértékü tagja a társadalomnak, hogy nem olvad be teljesen a közösségbe, nem oldódik fel a környezetében, saját maga vonja meg - a lehetőség és a társadalmi érdekek korlátai között - személyisége érvényesülésének a határait. Általában önállóan határozza meg azt az ismeretkört is, amelyen tul avatatlan szemek és fülek nem hatolhatnak. Ezt kivánja meg a személyes titok polgári jogi védelme. Ez azonban a számitógépes nyilvántartás területén csak korlátozottan érvényesül.

Korlátozások érvényesülnek a nyilvántartásba vétellel és a nyilvántartott adatok közlésével kapcsolatban.

A személyiségi érdekkört érintő adatok nyilvántartását az érintett személy hozzájárulása nélkül el lehet rendelni. Ilyen adatok közlésére azonban a személyt csak közérdekből, kivételesen lehet kötelezni. A természetes személyek adataira vonatkozó nyilvántartást csak a közérdekből valóban szükséges mértékre kell korlátozni. Ennek a biztositását szolgálja, hogy a jogszabály előirása szerint általánosságban ilyen nyilvántartást csak magasabb szintü jogszabály /törvény, törvényerejü rendelet, minisztertanácsi rendelet és határozat/ alapján és a felhasználó szerv felügyeletét ellátó miniszter engedélyével lehet elrendelni.

A Belügyminiszter 1/1981 /I.27./ BM. számu rendelete szerint viszont ilyen külön jogszabályi felhatalmazás nélkül is lehetőség van a munkaviszonybanm munka végzésére irányuló egyéb jogviszonyban álló személyek számitógépes nyilvántartására. Ilyen esetben a nyilvántartás feltétele csupán az, hogy a nyilvántartás a munkáltató szerv rendeltetésszerü céljaival

összefüggésben legyen, és a szerv vezetője engedélyezze. /21. § /2/ bek./

Ez a rendelkezés aggályosnak látszik, nem lehet a munkaviszony keretében a személyhez fűződő jogok védelmét szükebb körre szoritani, mint általában. A munkaviszony léte nem korlátozhatja a dolgozó személyiségi státusát, személyhez fűződő érdekeinek és jogainak a csorbitását, nem eredményezhet hátrányos megkülönböztetést. Ez a belügyminiszteri rendelet ellentétben áll az állami személyzeti munkáról szóló 1019/1974 /V.2./ Mt számu minisztertanácsi határozat rendelkezéseivel is, amely pontosan meghatározza, hogy a munkaviszonyban álló dolgozóról milyen adatokat lehet nyilvántartani. Nem teszi lehetővé általában a dolgozók minden olyan személyes adatának a nyilvántartását, amely "a munkáltató szerv rendeltetésszerü céljával összefügg", és amely adatok nyilvántartását a szerv vezetője elhatározza.

A számitógépes adatszolgáltatással kapcsolatban bizonyos fokig korlátozottan érvényesül a titok mással történő közlésére vonatkozó polgári jogi rendelkezés is, amely a személyes titok felfedéséhez, mással való közléséhez az érintett személy hozzájárulását teszik szükségessé. Általános szebály szerint a számitógéppel történő adatfeldolgozás nem sérthet személyhez füződő jogot. A titok megőrzésével kapcsolatban azonban a jogszabály annak az előirására korlátozódik, hogy a nyilvántartott adatokról tájékoztatást - az érintett személyeken kivül - csak az arra jogosult személyeknek vagy szerveknek lehet adni. Alacsonyabb szintü rendelkezések határozzák meg ezeknek a körét.

Egyébként a számitógépes nyilvántartással kapcsolatos - a nyilvántartott személyiségi jogait érintő titkot a Számitás-

technikai rendszerek titokvédelméről szóló 1/1981 /I.27./ BM. számu rendelet nem polgári jogi, hanem elsősorban államigazgatási, illetve büntetőjogi eszközökkel kivánja védeni.

Államigazgatási jellegü intézkedésként előirja, hogy a titkot képező adatok védelmét logikai-matematikai, illetve megfelelő technikai megoldásokkal is biztositani kell. Előirja, hogy a természetes személyekre vonatkozó nyilvántartást, feldolgozást, adatot szolgálati titokként kell kezelni. Egyes ilyen adatok államtitkot jelentenek.

Azokban az esetekben, amikor valamely személyt érintő titok államtitokként vagy szolgálati titokként államigazgatási, illetve büntetőjogi védelemben részesül, a titok polgári jogi védelmével kapcsolatos személyiségvédelmi rendelkezések gyakorlatilag háttérbe szorulnak. Az adatok mással való közléséhez nincs szükség az érintett személy hozzájárulására, az adatokat az erre külön feljogositott személyekkel, szervekkel közölni lehet. Nem az adhat engedélyt a titok felfedéséhez, közléséhez, akinek a személyére a titok vonatkozik, hanem az államigazgatási jellegü előirásokban meghatározott személyek és szervek.

A Ptk 83. §-a szerint is csak az államigazgatási szabályok szerint betekintésre nem jogosult személlyel, szervvel való közlés jelent jogsértést. A személy rendelkezési jogosultságának ez a korlátozása azonban nem jelenti, hogy a személyiségvédelem egyéb vonatkozásban is háttérbe szorul. A személyt érintő titok megismerésére, közlésére jogosult személyek meghatározásánál annak az érdekét is figyelembe kell venni, akire a titok vonatkozik, és a közlés kizárólag közérdekü célra történhet.

Egyéb vonatkozásban a titkot meg kell őrizni. Ez a rendelkezés azokat is köti, akik jogosultak a titkot jelentő adatok megismerésére. Nem eredményezheti az a közlés a titok megszünését. A titokvédelem köti azokat is, akik a nyilvántartás adatairól tájékoztatást kapnak, szerezhetnek. Az igy megszerzett titkot ezek is kötelesek megőrizni. /V.ö.: Dr. Törő Károly: Személyiségvédelem a polgári jogban./

Ebben a körben tekintettel kell lenni arra is, hogy mely adatok érintik a személyes titkot, mely adatok feltárása, másal közlése, nyilvánosságra hozatala jelent a polgári jog szabályai szerint titoksértést. Szükséges, hogy ezek az adatok valóban személyiségi érdekeket érintsenek. Az ilyen adatok felfedése, nyilvánosságra hozatala pedig csak akkor jogsértő, ha ezek az adatok egyediesitésre alkalmasak. Az egyediesitésre nem alkalmas statisztikai adatok közlése nem jelent jogsértést polgári jogi szempontból.

Gömbös Ervin:

AZ INFORMATIKA-POLITIKA NEMZETKÖZI VONATKOZÁSAI, TÖREKVÉSEK AZ INFORMATIKA SZABÁLYOZÁSÁRA

Bevezetés

Az információ a társadalmi cselekvőképesség egyre fontosabb hordozója. A kormányzati tevékenység, a gazdasági és tudományos élet, a társadalmi gyakorlat minden mozzanata megfelelő információt igényel. A vezetés és irányitás valamennyi területén és szintjén a helyes döntéseket csak a célszerüen összegyüjtött információk elemzésével és szelektálásával lehet meghozni. Ez önmagában nem uj jelenség, a társadalmi érintkezés mindig is információ-közvetitést jelentett. Az információ, mint társadalmi jelenség tulajdonképpen egyidős az emberiség történetével.

A XX. században kibontakozott társadalmi és gazdasági fejlődés, a termelés és a társadalmi élet valamennyi szférájának rendkivül bonyoluttá válása, a tudományos-technikai forradalom előrehaladása következtében azonban az információ "termelése", másrészt az iránta kialakult szükséglet oly mértékben megnövekedett, hogy kezelése, tárolása, közvetitése, illetve az igények kielégitése reménytelenné vált a hagyományos módszerekkel. A tudomány a feszitő társadalmi szükségletre ez esetben is válaszolt, mégpedig az elektronikus számitógépekkel.

A számitógépek fejlődésének példátlan gyorsasága - alátámasztva a mikro-elektronikával és összekapcsolva a távközléssel - azt eredményezte, hogy ma már az iparilag fejlett országokban a társadalmi tevékenység szinte valamennyi területén alkalmazzák. Elengedhetetlen eszköze az államigazgatásnak, a gazdaság irányitásának, a termelés hatékonyabbá téte-

lének, a nyersanyag és energia takarékosságnak, a kutató fejlesztő munkának, az orvosi ellátásnak, az oktatásnak, az adminisztrációs munka automatizálásának.

Az információs ipar, amely a fenti szükségleteknek megfelelő eszközöket és berendezéseket állitja elő, a fejlett tőkés országokban a leggyorsabban és legdinamikusabban fejlődő iparággá emelkedett, hamarosan olyan iparágakkal vetekszik, mint az olaj- és autóipar. Ezért a tőkés gazdaság egyik alapvető, élenjáró elemévé vált.

A számitógépesitás /összekapcsolva a távközléssel/ egy uj társadalmi jelenség, az informatika kialakulásához vezetett. Az informatika, mint diszciplina, az információ alkalmazását jelenti a társadalmi szükségletek kielégitésére, amelynek hátteréül az uj technika szolgál.

Az informatika társadalmi-gazdasági alkalmazásának és hatásának sokrétüségét - ezáltal politikai fontosságát - felismerve parlamentek, kormányok, tömegszervezetek, nemzetközi fórumok foglalkoznak az általa felvetett problémákkal. Belpolitikai jelentősége mellett mind fontosabb eleme lesz a külpolitikának is, az országok közötti - gazdasági, politikai és kulturális - kapcsolatok alakulásának.

A nemzetközi politikai vonatkozások elsősorban a nemzetközi adatforgalomból adódnak, amely a nemzetközi tőke, a multinacionális monopóliumok egyik uj eszköze versenyképességük növelése és befolyásuk bővitése érdekében. Mindez a fejlődő országok lemaradásának és kiszolgáltatottságának ujabb lehetősége, akik az uj nemzetközi információs rend megvalósitásáért küzdenek.

Számitógépek és távközlés[+]

A távközlés fejlődése lehetővé tette, hogy az egymástól elszigetelten müködő különféle számitógépeket - ezáltal a számitógépekkel kezelt információrendszereket is - összekapcsolják, hálózatba egyesitsék.
Lehetővé válik, hogy az ország bármely részén, sőt a külföldön lévő számitógépből is hihetetlenül rövid idő alatt kapjunk információt az ott tárolt adatokról.

A távközlés és a számitógépek társulása egy fejlődési folyamat eredménye - részben azért is, mert más és más a történetük és különböző a jellegük. A távközlés közel 150 éves multra tekinthet vissza, mig a számitástechnika alig 40 éves. Ezért a távközlés mint tudomány is sokkal megalapozottabb, mig a számitástudomány mégcsak fejlődésének kezdeti szakaszában tart. A távközlést szigoru - elsősorban nemzeti - előirások szabályozzák, magas foku szabványositás jellemzi. Ez tulajdonképpen azt jelenti, hogy kormányszintü döntések, irányelvek befolyásolják a távközlési rendszer kiépitését, müködtetését és fejlesztését. A számitástechnikára viszont a gyártók szabványai és politikája nyomja rá a bélyegét. Mivel a gyártás elsősorban a fejlett országok multinacionális vállalatai kezében van, igy azok nemzetközi befolyása, szabványmeghatározása dominál.

A számitógépek és a távközlés /beleértve a müholdat is!/ együttes rendszere arra utal, hogy a számitástudomány és a hirközlés elméleti határai mindinkább egymásba mosódnak: a azámitás- és átvitel-technikák - az utóbbiak digitalizálódásával és közös mikroelektronikai alapon fejlődve - összefonódnak és ezután un. távinformatika formájában terjednek, illetve ujulnak meg.

+ Távközlés alatt elektronikus eszközökkel történő információátvitelt értünk, történjen az akár digitális, akár analóg formában. Adatátvitel digitális információ /vagy adatok/ átvitele távközlési eszközök felhasználásával számitógépek és /vagy/ terminálok között.

A nemzetközi adatforgalom fogalma és szerepe

Az információs szektor kiépitése és különösen a technológiai fejlődés, amelyek a távinformatika alapját képezik, megteremtették a nemzetközi adatforgalom előfeltételeit. Ezt a fogalmat általánosságban ugy határozhatjuk meg, mint géppel olvasható adatok mozgása nemzeti határokon keresztül feldolgozás, tárolás, visszakeresés és felhasználás céljából. Ez a mozgás nemcsak távközlési csatornákon keresztül, hanem mágnesszalag, mágneslemez vagy más adathordozók szállitásával is történhet. Azonban egyre növekvő mértékben a távközlési vonalakat használják, amely feltételezi a megfelelő távközlési infrastruktura létét. Szükebb értelemben véve tehát a nemzetközi adatforgalom a tranznacionális számitógépes távközlési rendszereken keresztül történik.

Nemzetközi adatforgalom a távinformatika megjelenése előtt is létezett. Az uj technológia - a modern elektronikus adatfeldolgozási eszközök és a távközlési berendezések egyesülése - gyorsasága, az adatok közvetlen elérhetősége folytán megszüntette azokat a korlátokat, amelyeket az idő és távolság jelentett a nagytömegü információk mozgathatóságát illetően. A nemzetközi adatforgalom növekedését más tényezők is befolyásolják. Ezek közül első helyen kell emliteni a gazdaságot, amelyben egyre bővülő szerepe van az információs szektornak. Másrészt viszont más ágazatok fejlődése is mind inkább függvénye ennek a szektornak. További tényezők: a nemzetközi kereskedelem növekedése és olyan információ-igényes ágazatok nemzetközivé válása, mint a bankok, biztositás, turizmus és légiközlekedés, amelyek zökkenőmentes müködéséhez az adatok azonnali rendelkezésre állása és szétosztása szükséges. Meg kell még emliteni a mind nagyobbszámu multinacionális monopóliumot is, amelyek szintén ösztönözték a tranznacionális számitógépes távközlési rendszerek létrehozását. E nagy és bo-

nyolult - funkcionálisan különböző és földrajzilag szétszórt tevékenységeket folytató - szervezetek hatékony és eredményes irányitása, ellenőrzése és koordinálása nagytömegü adat gyors átvitelét követeli meg.

Nemzetközi adathálózatok

A nemzetközi adatforgalom infrastrukturáját - a számitógépek mellett - a távközlési hálózat jelenti. Kezdetben maga a telefonhálózat jelentette ezt, amely rendszerint állami tulajdonban van, szigoru kormányellenőrzés alatt áll. /Kivéve az Egyesült Államokat, ahol a telefonszolgáltatás 90 %-át két nagy monopólium - ATT és GTE - végzi./ A kontinensek közötti adatforgalmat - kétoldalu megállapodás alapján - első sorban nemzetközi távközlési monopóliumok látják el tengerfenéki kábeleken vagy müholdakon keresztül. Ezen berendezések többsége az északi féltekén van. A legfontosabbak az ITT Word Communiations, a RCA Global Communications és a Western Union Internacional magánvállalatok, amelyeknek saját kábelhálózata /és müholdjai/ vannak és ezek kapcsolódnak az egyes országok hálózataihoz.

A távközlési müholdak egy "földön kivüli" dimenziót vezettek be mind a nemzeti mind a nemzetközi adatforgalomba. A két nagy távközlési müholdrendszer az előzőekben ismertetett INTELSAT és INTERSZPUTNYIK. /Itt csak a távközlési müholdakkal foglalkozunk, a katonai - becslések szerint az összes müholdak kétharmada -, a légügyi és más kisérleti müholdak kivül esnek tárgykörünkön./ Más müholdrendszereket elsősorban hazai használatra - nagy monopóliumok közötti adatforgalom lebonyolitására - épitenek ki. Egyik ilyen rendszer, az amerikai Satellite Business System, 1981-ben kezdett müködni, fő felhasználói multinacionális monopóliumok. Hatóköre egyelőre csak az észak-amerikai kontinens, de a jövő-

ben más területekre is kiterjesztik. /A rendszer az IBM /41,3 %/, a COMSAT /41,3 %/ és az Aetna Life and Casualty /17,4 %/ tulajdona./

A távközlési hálózatoknak három alapvető tipusa van: /1/ - csak átvitelt megvalósitó alaphálózatok; /2/ - "értékkel növelt" hálózatok, amelyek az alaphálózatok vonalait bérlik és azt összekapcsolják saját számitógéprendszereikkel, igy az átvitel mellett más szolgáltatásokat is végeznek; /3/ - szolgáltató irodák, ahol a fő tevékenység az adatfeldolgozás és információvisszakeresés.

A hálózati végpontok /terminálok/ - ahol a tényleges felhasználás /adatlekérdezés/ történik - száma Nyugat-Európában hét év alatt 100 000-ről /1972/ 400 000-re /1979/ növekedett. Ez a szám 1987-re négyszeresére nő. A terminálok 3/5-e Nagy-Britanniában, NSZK-ban és Franciaországban van. Az Egyesült Államokhoz képest azonban ez még mindig alacsony szint, ahol 500 000-ről /1972/ 2 millióra /1979/ nőtt a hálózati végpontok száma. Ezer foglalkoztatottra számitva /1979/ az Egyesült Államokban 24,3, Nyugat-Európában 3,5 terminál van, tehát a különbség ugyanaz akkor is, ha nem abszolut számokban számolunk. Nyugat-Európában a legnagyobb nemzetközi adatforgalmat Nagy-Britannia, Svédország, Belgium, NSZK és Olaszország bonyolitja le, az egész háromnegyedét.

A legfejletlenebb európai tőkés országok - ahol a legalacsonyabb az egy főre jutó bruttó hazai termék - nemzetközi adatforgalma viszonylag magas. Ennek a magyarázata elsősorban az, hogy a hazai adatfeldolgozó kapacitás kicsi, igy kénytelenek az adatokat feldolgozásra exportálni és a feldolgozott adatokat importálni.

A nemzeti szuverenitás és biztonság

A számitógépek használata az államigazgatás és a gazdasági élet müködésének folytonosságát sokkal sebezhetőbbé tette, mint amilyen a számitógépek bevezetése előtt volt. Továbbá ezek a rendszerek egyre inkább egy szük szakmai rétegtől függnek, akik a programokat készitik, az adatbázisokat tervezik, a rendszereket müködtetik. A Svéd Honvédelmi Minisztérium jelentése szerint a "számitógépesitett társadalom sebezhetővé vált a számitógépes technológia és a számitógépes rendszerek meghibásodása, hiányosságai és rossz célra történő felhasználása következtében." A sebezhetőség csökkentése érdekében különféle technikai, technológiai védelmi eszközöket fejlesztettek ki. Emellett a legfontosabb a különféle u adatvédelmi törvények és jogszabályok bevezetése a számitógépes rendszerek müködtetésére vonatkozóan.

Az ország sebezhetősége természetesen növekszik,ha az adatfeldolgozást külföldön végzik és ezáltal az adatok országok közötti áramlására van szükség. A külföldön történő adatfeldolgozásnak lehetnek gazdasági okai /olcsóbb/, de olyan tényezők is szerepet játszanak, mint a szükséges hazai erőforrások /modellek, programok, adatbázisok vagy feldolgozó kapacitás/ hiánya. A külföldi adatfeldolgozási szolgáltatásokat használó országok fokozottan aggódnak a nemzetbiztonsági kockázatvállalás miatt és olyan általános kérdések miatt, mint a nemzeti önállóság, tekintély és függőség, amit röviden a nemzeti szuverenitással való törődésnek nevezhetünk. Az emlitett svéd jelentés igy fogalmaz: "A növekvő nemzetközi adatforgalom a biztonságnak és a sebezhetőségnek egészen más problémáit vet fel, mint amilyenek a tisztán nemzeti feltételek között léteznek. Ha az adatfeldolgozást egy másik országban vagy másik kontinensen lévő számitógépen végzik, és az adatok oda-vissza vitele több országon keresztül történik, a különféle jogelle

nes kezelés kockázata növekszik. A külföldi események elleni védekezés természetesen nehezebb, mint egy hazai védelmi rendszer kiépitése."

A szuverenitás az állam függetlensége az egyenlőség elve alapján minden más hatalommal szemben. Eszerint az állam saját területén minden személyre, testületre kiterjedő törvényes hatalmat gyakorol, más államok és nemzetközi szervezetek beavatkozásától mentesen. Önállóan irányitja politikai, gazdasági, társadalmi és kulturális életét és fejlődését. A nemzetközi adatforgalom bővülése fontos következményekkel járhat a nemzeti szuverenitás kérdését illetően is. Az alapvetően fontos döntéshozatali funkciók külföldre - az információban gazdag országokba - "vándorolnak". A nemzeti szuverenitást már az is sértheti, ha egy ország egy adott helyzetben nem ismeri az összes lehetséges alternativát, mivel nem fér hozzá a megfelelő információhoz. Ha egy ország keveset tud önmagáról és nemzetközi környezetéről - a szükséges adatgyüjtési és adatfeldolgozási rendszer hiánya miatt -, akkor a jövőjére vonatkozóan döntéshozatali lehetősége is korlátozott. Ily módon a nemzeti szuverenitás kiterjeszthető az "információs szuverenitásra" is.

A külföldi eszközökön és technológián - ezáltal külföldi információ-feldolgozáson - történő növekvő függőség csökkenti a hazai intézkedések lehetőségét üzemzavarok vagy más váratlan események /például sztrájk, számitógépes bünözés, személyi jogok megsértése/ esetén. Csökkenti a hazai szakmai követelményeket, ez pedig negativ hatással van a sajátosan hazai igényeknek megfelelő rendszerek kifejlesztésére.

A külföldön történő adatfeldolgozás és tárolás további lényeges problémája az is, hogy ilyen esetben szinte lehetetlen a

hazai jogszabályok érvényesitése egy másik országban történő tevékenységre. A multinacionális vállalatok leányvállalatai szinte kibujhatnak egy-egy ország joghatósága alól, mivel minden információs tevékenységük és ezáltal a döntéshozatal is az anyaországban - ahol a vállalat központja van - történik.

Valójában egyetlen ország sem lehet teljes mértékben önálló a szükséges információfeldolgozási szolgáltatások terén. Mindig szükség lehet speciálisan tudományos, ipari vagy gazdasági adatbankok elérésére vagy olyan adatfeldolgozási szolgáltatásra, amely az országon belül nem áll rendelkezésre. A növekvő kölcsönös függés - akárcsak más területeken is - elkerülhetetlen.

A nemzetbiztonsággal kapcsolatban olyan problémák vetődnek fel, mint a számitógépes rendszerek - földrajzi és funkcionális - koncentrációja. Az országok többségében e rendszerek 70-80 %-a néhány nagy városban van. Háboru esetén ezek védelme a lerombolástól, vagy ellenséges célokra történő felhasználástól különös gondot jelent. Feszült nemzetközi légkör esetén nehéz a külföldi berendezések zavartalan üzemeltetése /pl. alkatrész utánpótlás elmaradása miatt/, háboru idején pedig fokozottabb veszélyt jelenthet. A külföldön tárolt információt felhasználhatják katonai, stratégiai célokra. További problémát jelenthet - békés időszakban is - a szomszédos országok politikai stabilitásának megrendülése, amelynek következtében bizonyos időre lezárhatják a távközlési vonalakat, vagyis az adathálózatoknak az országon átvezető részét. Müholdakon keresztül történő átvitel esetén ez nem probléma, de a müholdakat is meg lehet semmisiteni.

Bizalmas jellegü adatok külföldön - különösen olyan ország-

ban, ahol adatvédelmi törvények nincsenek - történő feldolgozása kézenfekvő hatással lehet az országra és lakosaira is. Például, ha névvel ellátott adatokat juttatnak ki az országból. Az ilyen és hasonló esetek az országgal és lakosaival történő manipulációra és más veszélyes cselekményekre adhatnak lehetőséget.

A nemzeti szuverenitás és biztonság kérdése egyaránt érinti mind a fejlett, mind a fejlődő országokat. Egyre több - elsősorban fejlett - országban foglalkoznak kormány vagy parlamenti szinten a szükséges jogi és egyéb védelmi intézkedések kidolgozásával. Számos adatvédelmi törvényt alkottak a nemzetközi adatforgalom szabályozására, a nemzeti érdekek védelmére. Ki kell emelni Svédországot, Franciaországot és Kanadát, amelyek elsőként foglalkoztak a legmagasabb szinten e kérdéskörrel. Mindhárom esetben az Egyesült Államok és multinacionális vállalatai /pl. IBM/ kihivása és egyeduralma ellen, függőségük csökkentése érdekében tettek kezdeményező lépéseket.

Az emlitett svéd jelentés azt a következtetést vonta le, hogy az ország sebezhetősége e területen rendkivül magas - többek között a külföldi erőforrásoktól való függés miatt - és a továbbiakban ez még nő, ha megfelelő ellenintézkedéseket nem tesznek. Egyik ilyen intézkedés lehet a számitógépesités engedélyeztetése az egész közigazgatásban /kivéve a honvédelmet/.

A kanadai Távközlési Minisztérium által létrehozott bizottság jelentése /Telecommunication and Canada, 1979./ többek között az alábbi veszélyekre hivta fel a figyelmet, amelyek a külföldi - elsősorban amerikai - számitógépes szolgáltatások növekvő használata és azoktól való függés következtében előállhatnak:

- növekszik annak lehetősége, hogy Kanadában titkos információt külföldön nyilvánosságra hozzanak;
- veszélybe kerül a kanadai igazságszolgáltatás gyakorlása a Kanadában müködő vállalatok felett, amelyek külföldön tárolják és dolgozzák fel adataikat;
- lehetővé válik, hogy - a külföldi adatbankokra épülő - Videotex szolgáltatások külföldi értékeket, árukat és szolgáltatásokat helyezzenek előtérbe;
- az Egyesült Államok kormányának könnyebb lesz kisérletet tennie arra, hogy törvényeit saját területén kivül is alkalmazza.

A bizottság jelentése azt ajánlja a kormánynak, hogy országos felvilágositó kampányt kell inditani: megmagyarázni az "uj elektronikus információs társadalom" gazdasági, társadalmi és kulturális következményeit. A kanadai vállalatok adatfeldolgozását végezzék Kanadában, kivéve ha engedély van külföldi feldolgozásra. A kormány tiltsa meg, hogy a bankok és biztositó társaságok ügyfeleire vonatkozó adatokat külföldön tároljanak és dolgoztassanak fel. Támogassa jobban a kanadai információs ipart és hatékonyabb szakemberképzést valósitson meg. Végül azt javasolja, hogy "a kormánynak sürgősen szabályoznia kell a nemzetközi adatforgalmat, hogy ne veszitsük el ellenőrzésünket a nemzeti szuverenitás megtartásához létfontosságu információ felett."

A kanadai Távközlési Minisztérium miniszterhelyettese, Bernard Ostry egyik beszédéből /1979-ben/ való az alábbi idézet: "Képzeljék el a jövőt, amikor az információ géppel olvasható formában kell, hogy legyen, hogy minél szélesebb körben terjeszthessék. Mi történne, ha csak külföldi nagyvállalatok és kormányok transzformálnák az információt gép-

pel olvasható formába; Kanadáról - területéről, irodalmáról, jogrendszeréről, történelméről, hagyományairól - mennyi információt kapnának a Kanadaiak? És melyik hivatalos nyelvünkön? Valószinüleg nagyon keveset. Egy ilyen jövőben nem ismernénk magunkat, és gyorsan megszünnénk létezni, mint a kanadai nemzet."

A társadalom informatizálásáról Franciaországban készitett Nora-Minc jelentés a nemzeti szuverenitás vonatkozásában egyaránt negativ hatásunak tekinti a külföldön történő adatfeldolgozást és adatbázis szolgáltatások igénybevételét, valamint az importált adatfeldolgozási berendezések és /vagy/ szoftver használatát. A jelentés megállapitja, hogy Franciaországban az információs forradalomnak sokkal messzebb menő következményei lesznek, mint az ipari forradalomnak volt, és teljesen megváltoztatja a társadalom lényegét és szervezeteit. A jelentés azt bizonyitja, hogy ezt a forradalmi változást - amely a távinformatika következménye - a franciáknak maguknak kell irányitaniuk a távinformatikai alkalmazások és rendszerek kiépitésén, müködtetésén és ellenőrzésén keresztül, beleértve az "IBM kihivásának" megujulását.

A fejlődő országok többek között az IBI+ által szervezett első nemzetközi /SPIN/ konferencián megállapitották, hogy "bármely országnak, amely szuverén akar maradni függetlenné kell válnia az informatikában." Az informatika fejlődése által a nemzetközi kapcsolatokban felmerülő kérdések közül az egyik legfontosabb kérdés a nemzetközi adatforgalom, amely veszélyeztetheti a nemzeti szuverenitást, ha titkot képező vagy személyekre vonatkozó információ külföldre kerül.

+ Kormányközi Informatikai Iroda /Intergovernmental Bureau for Informatics, Róma/

Törekvések a nemzetközi adatforgalom szabályozására

Az információ fontosságának növekedése, továbbá a nemzetközi adatforgalom politikai, gazdasági, szociális és kulturális hatásának fokozott mértékü felismerése számos kormányt arra ösztönöz, hogy megfelelő választ adjon erre a jelenségre. A távinformatika és a nemzetközi adatforgalom elsősorban a fejlett tőkés országokban, illetve azok között fejlődött ki legszélesebb körben, legnagyobb tapasztalattal azok rendelkeznek, igy a jelentkező problémák megoldásának igénye, megfelelő szabályozás kialakitásának szükségessége is náluk vetődött fel először. Az adatforgalmat szabályozó irányelvek és jogszabályok kialakitása mind nemzeti, mind nemzetközi szinten még csak a kezdetnél tart, kivéve a személyekre vonatkozó adatok nemzetközi forgalmát, ahol már jelentős, konkrét intézkedések történtek. Az ilyen jellegü adatokkal kapcsolatos, személyekhez füződő jogok védelme egyben ráirányitja a figyelmet a nemzetközi adatforgalom általános kérdéseire, ezáltal a nemzeti és végsősoron nemzetközi szabályozások kialakitását idézi elő.

A nemzetközi adatforgalom további problémákat vet fel a személyi jogok védelmét illetően. Ilyen vonatkozásban már nem elegendő biztositék a hazai jogszabályalkotás, mert az nem védi a külföldre kivitt, ott tárolt és feldolgozott adatokat. A nemzetközi adatforgalmat illetően az adatvédelmi törvények fő célja elsősorban nem önmagában az adatforgalom szabályozása, hanem inkább annak biztositása, hogy egy adott országból származó adatok az adott ország adatvédelmi jogszabályai alá essenek, függetlenül attól, hogy a feldolgozás, a tárolás és visszakeresés hol, melyik országban történik. Ausztriában például a személyi adatok védelmére - 1978 októberében - hozott törvény előirja, hogy az Adatvé-

delmi Bizottság engedélye szükséges az adatok exportjához, kivéve többek között, ha az adatok olyan országba kerülnek, ahol azokat hasonló módon védik, mint Ausztriában. 1981-ben egy külön rendelet határozta meg ezeket az országokat: Dánia, Franciaország, NSZK, Luxemburg, Norvégia és Svédország. A kereskedelmi jog által meghatározott jogi személyekre és társulásokra - amelyek székhelye Ausztriában van - vonatkozó adatok esetén a fenti kör szükebb, mivel ez esetben engedély szükséges, ha Franciaországba, NSZK-ba vagy Svédországba történik kivitel. Minden esetben engedélyhez kötött az adatok kivitele, ha azokat várhatóan re-exportálják olyan országba, ahol nincs érvényben ugyanolyan adatvédelmi törvény, mint Ausztriában. Olyan adatok esetén, amikor a küldő csak önmagára vonatkozó adatokat akar exportálni, nincs szükség az engedélyeztetésre.

A 23 OECD tagállam közül 1981 elején 12 országban volt érvényben adatvédelmi törvény vagy kormányszintü rendelet. Néhány más országban előkészületben van, de valamennyi tagállamban foglalkozott a kormány az elmult években a kérdéssel, ott is, ahol jogszabály még nem született.

Nemzetközi szintü kormányközi szervezetek közül az Európa Tanács miniszteri bizottsága fogadta el "A személyi adatok automatikus feldolgozásával kapcsolatos személyi jogok védelmére vonatkozó egyezményét" 1980 szeptemberében, amely ratifikálás után kötelező érvényü az aláirókra nézve. Ugyanebben az időszakban - öt nappal később - az OECD Tanácsa "A személyi adatok nemzetközi forgalmát és a személyi jogok védelmét szabályozó irányelveket" fogadott el /Ausztrália, Kanada, Izland és az Egyesült Királyság ezt nem irták alá./ A fenti szervezetek mellett az Európa Parlament is foglalkozott a nemzetközi adatforgalommal. 1979 májusában határoza-

tot hozott a személyi jogok védelmére, tekintettel az adatfeldolgozás területén végbemenő technikai fejlődésre. Sem az OECD irányelvei, sem az Európa Tanács határozata nem kötelező érvényü, csupán javaslatok a tagországok számára.

A fejlett tőkésországok adatvédelmi törvényei és rendeletei mind hazai, mind nemzetközi adatforgalom vonatkozásában elsősorban a személyi jogok védelmére koncentrálnak, legyen szó akár természetes, akár jogi személyekről. Az uj technológia hatása számos ország esetében azonban messze tulnő ezen a problémakörön, sokkal fontosabb és érzékenyebb területeket érint, nevezetesen a gazdasági fejlődést és a nemzetközi kapcsolatokat. A nemzetközi adatforgalomban az adatok jórésze - személyi jellegü - természetes vagy jogi személyekhez kapcsolódó. Az ezekre vonatkozó szabályozások sok esetben az egyéb adatok védelmét is érintik, vagy legalább is hatással vannak arra. Kanadában például külön rendelet szabályozza a gazdasági adatbankok létrehozását és müködtetését - elsősorban a nemzeti érdekek biztositása és védelme céljából.

A gazdasági fejlődést, a nemzetközi kereskedelmi és egyéb kapcsolatokat érintő kérdéseket, amelyek a távinformatika alkalmazásából erednek, megfelelő informatika-politika kialakitásával és érvényesitésével szándékozik számos ország megoldani. Körülbelül 60 ország fogadott el hivatalos informatika-politikát, amelyek jelentős része az adatfeldolgozási berendezések gyártásával, beszerzésével, használatukkal kapcsolatos prioritások meghatározásával, valamint az alkalmazásokkal foglalkozik. Közvetve vagy közvetlenül ennek a politikának hatása van a nemzetközi adatforgalomra is. Esetenként konkrét szabályozásokat is bevezetnek. E téren ki kell emelni Kanadát, Svédországot, Franciaországot és Brazi

liát. Ezen országok esetében az informatika-politika közös jellemzője az amerikai multinacionális monopóliumok befolyásának korlátozása és visszaszoritása, amelyek a technológia, a gyártás, az alkalmazás, valamint a nemzetközi adatforgalom és infrastrukturájának gyakorlatilag valamennyi területén tulsulyban vannak.

Az Egyesült Államok és a nemzetközi adatforgalom

A nemzetközi adatforgalommal kapcsolatos kérdéseket és problémákat először néhány tőkés ország /Svédország, Franciaország, Kanada/, majd a fejlődő országok vetettek fel, vitték nemzetközi fórumok elé /UNESCO, IBI/. Az egyre élesedő nemzetközi nyomás arra kényszeritette az Egyesült Államokat, hogy kormányszinten foglalkozzon a kérdéssel annál is inkább, mivel a támadás több irányból is jött, továbbá több szempontból is érintette.

Az Egyesült Államoknak van a világon a legnagyobb távközlési hálózata, beleértve a müholdas rendszereket is. Az Egyesült Államok a világ legnagyobb információ gyüjtője, tárolója, feldolgozója és szétosztója. A távközlési és számitástechnikai berendezések évi amerikai exportja 5 milliárd dollár, amellyel a nemzetközi nem szocialista piac 80 %-át tudhatja magáénak. Mindezt néhány multinacionális monopólium bonyolitja le, élükön az IBM-mel.

Az amerikai politika alapvető célja a helyzet konzerválása, egyeduralmának megtartása, illetve bővitése. Kormányszintü kidolgozását Carter elnöksége idején kezdték, szorosan összekapcsolva az "információk szabad nemzetközi áramlását" az emberi jogok kérdéseivel, a külpolitika központi elemével. Ebben az időszakban hozták létre a Nemzeti Távközlési

és Információs Igazgatóságot /National Telecommunications and Information Administration - NTIA/ és a Nemzetközi Kommunikációs Ügynökséget /International Communications Agency ICA/.

Carter elnök a Kongresszusnak készitett beszámolójában /1977. január/ kijelenti, hogy az Egyesült Államoknak "nemzetbiztonsági, politikai, ideológiai, gazdasági és technológiai érdekei vannak a nemzetközi kommunikációban", és a "nemzetbiztonság a fejlett távközlési rendszerektől függ." A továbbiakban igy fogalmaz: "Gazdasági érdekünk nyilvánvaló: ipari bázisunk a megfelelő kommunikációra épül; a nagy vállalatok egyre inkább függnek az egész világra kiterjedő számitógépes hálózatoktól."

Az Egyesült Államok eddigi befolyásának megőrzése és bővitése érdekében vagyis multinacionális monopóliumai érdekeinek védelmében a status quo megőrzésére törekszik. Ragaszkodik ahhoz, hogy a nemzetközi adatforgalomban is ismerjék el az olyan alapelveket, mint az információ szabad áramlása, szabad vállalkozás, szabad kereskedelem, és vegyék figyelembe a szükséges távközlési eszközök és szolgáltatások megfelelő rendelkezésre állását. Ezt tükrözte Matthew Nimetz, amerikai külügyminiszterhelyettes előadása is az OECD által 1980 októberében Párizsban szervezett; "A 80-as évek információs, számitógépes és kommunikációs politikáját" tárgyaló magasszintü konferencián.

Barry M. Goldwater Jr. amerikai szenátor informatikai szakemberek előtt tartott előadásában kijelentette, hogy a nemzetközi adatforgalom egy olyan fontos kérdés, amelyet ha nem oldanak meg rövid időn belül, gyengitheti az amerikai ipar versenyképességét és előnyét a külföldi piacokon. Tá-

madta a francia adatvédelmi törvényt, amely megtiltja az adatok külföldre vitelét engedély nélkül. Szerinte ez azt is jelenti, hogy csak francia számitógépeken keresztül történhet az adatok kivitele, amely az amerikai számitógépipar érdekeit is sérti. Akárcsak a legtöbb amerikai politikai vagy gazdasági vezető, kiállt az információ szabad áramlása mellett, amely - mint mondotta - "a gazdaságunk müködéséhez szükséges kenőolaj."

Az információáramlás termelés és termelékenység növelési képessége, valamint a piaci viszonyok gyors felmérése révén jelentős hasznot hozó erőforrás a multinacionális monopóliumoknak. Ezért elleneznek mindenféle nemzeti autoritást, vagy érdemleges nemzetközi ellenőrzést az információáramlás felett. Az amerikai gazdaság hagyományos erőforrása: teljesitőképesség, a kiváló technológiai ismeret és a katonai hatalom. Vezetői napjainkban egyre nagyobb jelentőséget tulajdonitanak a kommunikáció ellenőrzésének is. Az a nagyarányu információáradat, amelyet az amerikai monopóliumok külföldön létrehoznak és támogatnak, erőteljesen hozzájárul érdekeik hazai fenntartásához és globális kiterjesztéséhez.

Weisz Istvánné dr.:

AZ ADATVÉDELEM UJ VONÁSAI ÉS AKTUÁLIS KÉRDÉSEI

Az adatvédelem uj vonásairól a végrehajtási utasitások megjelenése kapcsán beszélhetünk. Ez a szakasz a rendelet hatályba lépése óta eltelt, közel 2 éves periódust öleli fel és jelzi, hogy bizonyos célszerüségi és gyakorlati tapasztalatok kialakulóban vannak, amelyre a jogalkotásnak is helyes felfigyelnie.
E fogalmomkörbe a következő kérdések sorolhatók:

- A személyi adatbankokkal kapcsolatos jóváhagyási eljárásnál rögzitett "szerzett jogok" intézménye kialakitotta, illetve feltehetőleg folyamosan alakitja a természetes személyekre vonatkozó számitástechnikai feldolgozások tárcaszintü regisztrációját.
  Erre a folyamatra feltétlenül gondot kell forditani. Egyrészről ugyanis - ha ágazatközi szinten ezt kellően kezelik - a párhuzamosságok kiszürésére, az adatcserék kialakitására komoly lehetőségeket ad. Másrészről a személyi jogok védelmével kapcsolatos szabályozás, elemzés, értékelés szempontjából felbecsülhetetlen mértékü adat- és tényhalmazt képes nyujtani, szükségtelenné téve a becslést, a modellezést.

- Bizonyos polarizálódás tapasztalható a "számitástechnikai eszköz" terminológiájának alakulásában. A meghatározások egy része az ide vonatkozó magyar szabvány oldaláról közelit, de használatos az operációs rendszerrel való müködtetés - mint feltétel - kikötése is. Ehhez kapcsolódik - mindkét irányu definiciónál - az "egyszerü eszközök" fogalmának bevezetése, amelyeknél az előirások szigora általában mérséklődik. E körben emlithető a távadatfeldolgozás bizonyos szükitett értelmezése is.

- A fenti témával szoros és logikus kapcsolatban jelent meg az "egyszerüsitett SZVSZ" /Számitástechnikai Védelmi Szabályzat használatos röviditése/ intézménye, amely a számitástechnikai rendszerhez rendszerfunkciókkal nem kapcsolódó egyszerü eszközök szabályozási metodikájára nézve tartalmaz könnyitéseket.

- A célszerüséget, a reális kockázatvállalást, nem utolsósorban a gazdaságosság tényezőit segiti az adatvédelmi mechanizmusban a "differenciált SZVSZ" megjelenése. Lényege, hogy azonos jogi személyen belül többféle biztonsági fokozat is érvényesülhet, amennyiben helyileg elkülönülő számitástechnikai egységek léteznek, olyan jól definiált rendszerfunkciókkal, amely a kezelés különbözőségét szakmailag és jogilag egyaránt megalapozza. Természetesen ilyen gyakorlat több SZVSZ elkészitését tételezi fel.

- Bár nem jellemző, de megemlitendő, hogy a magánszemélyeknek minősülő társaságok kizárása is előfordul titkos adatkörrel való munkavégzésből, noha a rendelkezések csak megkülönböztetett kezelést irnak elő. E módszer valóban ad egy nagyfoku biztonságot, azonban az együttmüködési, munkavégzési kapcsolatokat merevitheti, és indokoltsága vállalati gazdasági munkaközösségek esetében megkérdőjelezhető.
  Egyébként még nem kellően tisztázott elvi kérdés, hogy a közös néven megjelenő és közös képviselő által képviselt, ilyen társaságok esetében mennyiben és milyen módszerekkel és lehetőségekkel vizsgálható a tagokra vonatkozóan a feladatok biztonságos teljesitésének kérdése.

- Rendkivül figyelemreméltó az a lehetőség, hogy a szervvel munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló természetes személyek jogszerü tartalommal

folyó adatfeldolgozása, nyilvántartása stb. önmagában nem eredményez fokozott biztonsági kategóriát. Erre az Irányelvek megfelelő alapot nyujt. Célszerü, sőt igen lényeges lenne ennek az elvnek az átvétele a központi szabályozási körbe, egyben - a realitásokat mérlegelve - annak tisztázása, hogy az ilyen adatokat hivatásszerüen számitástechnikai eszközzel feldolgozó szervekre e kedvezményezett módszer kiterjeszthető-e, megfelelő szerződési garanciákkal való felváltás esetén. Ez már üzletpolitikai szempontokat is érintő kérdés.

- Kialakult némi bizonytalanság a fontosabb felhasználóhelyeken való teendők tekintetében. Egyes szervek, intézmények - bár rendeletileg erre nem kötelezettek - felhasználói SZVSZ-eket dolgoznak ki, illetve ilyent terveznek, amelyekben a hangsuly általában a futó, vagy tervezés alatt álló rendszerek analizisén és a külső kapcsolatok elvárási szempontjain van. E kérdésre nézve a végrehajtási utasitások nem foglaltak állást, nem teremtettek egységes gyakorlatot. Tekintettel arra, hogy az adatvédelem a számitástechnika alkalmazása teljes folyamatára vonatkozik, e probléma átgondolást, megfontolást igényel és célszerü lenne a technológiai sor lényeges elemét jelentő felhasználókat is bevonni - valamely egyértelmü metodika szerint - a szabálvozás körébe.

A jövő tennivalóit és feladatait áttekintve megállapitható, hogy vannak sürgetően aktuális és ugyanilyen fontos, de távolabbi, illetve perspektivikus megoldandó kérdések.
Ezek egy része szakmai, szervezési, más része szabályozási, illetve elméleti megalapozást is igénylő témakör.
Csak a legfontosabbakat emlitve:

- A belügyminiszteri rendelet szerint a jogszabályi hierarchia magas szintjén álló, de legalább minisztertanácsi

határozatban rögzitett felhatalmazás szükséges ahhoz, hogy a miniszter ágazata területén természetesen személyeket érintő számitástechnikai adatfeldolgozást /stb./ engedélyezhessen. Ennek algoritmusa azonban tisztázatlan. Ugyanigy vizsgálatot igényel az, hogy e hivatkozott jogszabályokban előforduló feladatmeghatározások, a feldolgozással kapcsolatba hozható, de általános megfogalmazások mennyiben tekinthetők egy adott, konkrét ügy jogszerü engedélyezési alapjának.

- A végrehajtási utasitások elég jelentős része áll még megjelenés előtt. Célszerü lenne, ha az egyes tárcáknál érvényesitett, de közérdeklődésre számot tartó, ujszerü intézmények e forrásokban már megjelennének. Ennek hatékony ösztönzési módja lenne, ha a kiadás előtti véleményezésnél ezek érvényesitésére sor kerülne.

- Az adatvédelem az érdeklődés homlokterébe került, de igen kevés még a tapasztalati alap. Abban szinte valamennyi végrehajtási utasitás egyöntetü, hogy effektiv gyakorlati eszközökre vonatkozó iránymutatást nem ad. Emellett e kérdésnek nincs kialakult intézményrendszere. Mindezek áthidalására jelenleg - első lépésként - akár hivatalos, akár társadalmi alapon javasolnám egy adatvédelemi eszközbank létrehozását, önkéntes alapon és szabad hozzáféréssel. Ez az eszközbank egyaránt tartalmazna terminológiákat, technológiai eljárásokat, fizikai eszközök megnevezését és leirását, szellemes megoldásokat, hasznos módszereket, közérdekü tipuselemeket, s természetesen mindezeket kifejezetten az adatvédelemre specializálva. Nyilvánvaló, hogy az adatfelvétel, a tárolás, a hozzáférés módja, mindezek ügymeneti kérdései még átgondolást igényelnek, de a megvalósitás kétségtelen társadalmi hasznossága megéri a ráforditott energiát.

A szabályozás továbbfejlesztése, az elméleti tisztázás irányába mutatnak azok a még megoldásra váró témák, amelyek a több éve megkezdődött és több, mint két éve lezárult rendeletelőkészitési szakaszban még nem, vagy nem ezzel a sullyal jelentkeztek.
Ezek közül is csak néhányat kiemelve:

- A személyi adatnyilvántartásokkal /stb./ kapcsolatban három alapvető kérdést a jelenlegi szabályozás nem kezel. Miután adatvédelmi szeppntból ezek neuralgikus pontok, vizsgálatuk aktuális lenne. A problémakörök
  = a rendszerbővitések
  = a rendszerösszakapcsolások
  = és a rendszerekből való szolgáltatás kérdései.

  Mindhárom ügyben elég nagy bizonytalanság alakult ki a gyakorlatban.

- Ugyancsak kimunkálásra vár a jogvédelem tekintetében a jogi személyekre vonatkozó eljárások szabályozása.

- Tisztázásra várnak az adatvédelem előirásainak egyes nemzetközi vonatkozásai, amelyeket jelentőssé tesznek az egyre szignifikánsabb szerepet kapó nemzetközi kapcsolatok hatásai. Gondolok itt elsősorban a magyar intézmények partnerkörébe megjelenő külföldi természetes és jogi személyekre, illetve a Magyarországon lévő külföldi intézményekre, az ezekkel kapcsolatos hatálybeli és eljárásbeli specifikumokra, illetve a nemzetközi adatforgalomra.

- A minősitési rendszerek átgondolását igényli a differenciált SZVSZ-esk analógiájára felmerülő "szelektiv adatvédelem" problémaköre. Racionális, gazdasági, praktikus szempontból egyaránt jelentkezik ugyanis az az igény, hogy egy adott rendszeren belül különböző minősitésü, s igy eltérő biztonsági igényü adatkörök is megjelenhessenek,

valamiféle moduláris elvből kiindulva. Megoldása mind szakmai, mind biztonsági oldalról kiván lépéseket.

- Fel kell készülni a számitástechnikai eszközpiacon megjelenő és merőben uj technológiai folyamatokat generáló eszközökre, azok beépitésére az adatvédelem rendszerébe. Emellett is még tisztázásra várnak bizonyos hagyományos terminológiai kérdések, pl. olyan, látszatra sztereotip fogalom, mint a sokszorositás, is gondokat okoz számitástechnikai környezetben, titkos adatkörnél. Hasonló a helyzet a minősitő jelzés alkalmazásával kapcsolatos problémákkal, pl. különösen nagy tömegü, papiralaku adathordozók esetén.

- Végezetül különösen jelentős kérdésnek tartom, hogy a jelenlegi jogrendszerünkben meglévő, különböző szintü, megközelitésü, de alapvetően azonos célt szolgáló jogi rendezés az adatvédelem területén összehangolódjék, természetesen nem azzal az igénnyel, hogy a speciális védelmek megszünjenek, hanem kizárólag annak érdekében, hogy egymásra tekintettel létezzenek. /Pl. statisztikai adatok védelme, az állami népességnyilvántartás rendszerével kapcsolatos külön szabályok, etikai védelem, az általános titokvédelmi rendszer és annak a legutóbbi időkben nagy számban születő specializálásai és mindezek jelentkezése a számitástechnikai adatvédelemben./

Ugy vélem, fentiekből körvonalazódott az a kétirányu tendencia, amelyet a számitástechnikai adatvédelem megjelenése óta eltelt időszakban érzékelni lehetett.
E két tendencia: egyoldalról a gyakorlati végrehajtás segitésének, a konrét módszerek és eszközök kimunkálásának, illetve elterjesztésének igénye, s ezzel a már hatályos rendezés megalapozása szakmai szempontból, más oldalról e

rendkivül dinamikus technológiával párhuzamosan az adatvédelmi szabályozás folyamatos karbantartása, igazitása a müszaki, technikai és egyéb infrastrukturális követelményrendszerhez, nem utolsósorban még nem tisztázott problémák elméleti megalapozása és ennek utján a szabályozás továbbfejlesztése.

Bizom benne, hogy mindkét irány kellő támogatásra lel.

dr. Kondricz József:

KORREFERÁTUM A SZÁMITÁSTECHNIKAI ADATVÉDELEM' 1982. RENDEZVÉNYÉRE

Vállalati politikánk egyik eleme a biztonság. Ez egyrészt ügyfeleink gyors, pontos határidőre történő megbizható korrekt kiszolgálását jelenti, másrészt leegyszerüsitve fogalmazva a "biztonság pénz", amelyben ugy gondolom sok igazság van igy is, ugy is. Nagy értéket képvisel egy biztonságosan üzemeltethető adatfeldolgozási rendszer. Jelentős összegbe kerül a korszerü hardware eszköz, valamint a megbizható védelemmel felszerelt software beszerzése és a jól kiképzett munkaerő biztositása.
A számitástechnikai tevékenység biztonságának megvalósitása pénz igényes, mert mind az, amely a számitógépes rendszer folyamatos és zavartalan müködéséhez valószinüségét növeli, az a másik oldalon fokozza az anyagi és a szellemi erőforrások igénybevételét. Ezért a számitástechnikai rendszerek védelmének kialakitásánál figyelembe kell venni a védelem hiányosságából adódó kár és a védelem megvalósitásához szükséges költségek egymáshoz való viszonyát.

Üzleti kapcsolataink gyakorlatában mindig fontos tényezőnek tekintettük a számitástechnikai rendszerek biztonságtechnikai feltételeinek kialakitását. Ugyanakkor erősen vitatható volt, hogy megtett intézkedéseink megfelelnek-e az elvárható minimális követelményeknek. Az adatvédelem megvalósitásában milyen feladat hárul az üzemeltetőre és milyen a felhasználóra. Ki állapitja meg a számitástechnikai rendszerek feldolgozása során keletkezett adatok minősitését, a védelmi eljárások szükségességét és mértékét. A számitástechnikai rendszerek titok-, vagyon- és tüzvédelméről szóló 1/1981. /I.27./

BM számu rendelet, valamint az alapján megjelent 4/1982./ /SK7./ KSH számu utasitás a korábban erősen vitatható kérdésekre egyértelmü feleletet ad.
Egységesiti a biztonság megvalósitásával kapcsolatos fogalmak tartalmát, a védelmi eljárások elvárható követelményét. Utasitást ad az üzemeltető részére a Számitástechnikai Védelmi Szabályzat elkészitésére és gyakorlati alkalmazására.

Az SzVSz-ben a rendeletnek és az utasitás előirásának megfelelően szabályozzuk vállalatunknál az államtitoknak és a szolgálati titoknak minősülő adatok számitógépes rendszerben történő feldolgozásának teljes technológiai folyamatát, a biztonsági okokból előállitott másolati adathordozók biztonságos körülmények között történő megőrzését. /Ha felmerül./

Felhasználóinkkal közösen gondoskodunk az államtitoknak, vagy szolgálati titoknak nem minősülő minden más adat védelméről.

Korreferátumomban röviden fel szeretném vázolni azokat a feladatokat, amelyek egy számitástechnikai bérszolgáltatást végző országos hálózattal rendelkező vállalatra hárulnak a számitástechnikai rendszerek titok-, vagyon- és tüzvédelméről szóló BM rendelet, illetve annak végrehajtására kiadott KSH elnöki utasitás alapján.

Feladataink megvalósitása ezen a területen jelentős mértékü anyagi kiadásokkal is jár, munkatársainktól pedig bizonyos mértékig szemléletváltozást és fegyelmezettebb, jobban felkészült munkát is igényel.

Vállalatunknál több mint 30 db számitógépet üzemeltetünk, kö-

zel 500 adatrögzitő hellyel rendelkezünk, a hálózatunkban foldolgozott témák száma meghaladja az 1000-et, és megrendelőink száma eléri a 660-at.
Ezzel az eszközháttérrel kell megoldanunk a 660 megrendelő részére a biztonságos számitástechnikai feldolgozásokat.

Feladatainkat a vállalati irányitás mellett 18 szervezeti egységnél, 17 telephelyen látjuk el.
Árbevételünk megközeliti az 1,2 milliárd forintot, foglalkoztatottjaink száma pedig 3487 fő.

Olyan országos megrendelőkkel állunk kapcsolatban, amelyeknél a titoktartást államilag is szavatolják, gondolok itt az OTP feldolgozásokra, vagy olyan pénzintézetekre, amelyeknek a teljes ügyviteli feldolgozása már most, vagy a közeljövőben a hálózatunkban üzemel, pl. Állami Biztositó feldolgozása, a biztositásokkal kapcsolatos nyilvántartások köre. De nem utolsó sorban emlitem meg a vállalati gazdálkodást folytató szervezetek részére végzett számitógépes feldolgozásainkat, az azokhoz kapcsolódó üzemi titkok betartásának biztositását.

A biztonsági előirások kialakitását és megvalósitását tovább szélesiti, illetve bonyolitja a távadatfeldolgozásaink, valamint a COM szolgáltatásaink fejlesztése, a külső megrendelők részére végzendő szerviz tevékenység kialakitása, a megyeszékhelyeken kivüli adatrögzitői kirendeltségek müködtetése, a különböző együttmüködési formákban kialakitott szervezeti egységek üzembiztonságának a megvalósitása.

A felsorolt körülmények között ugy gondolom, nem jelent könnyü feladatot az előirt feladatok vállalaton belüli feltételeinek a kialakitása.

Nagyon sok időt kötött le az, hogy az egyes előirásokat hogyan és milyen formában kell érvényesiteni vállalatunknál.

Sokáig kérdéses volt, hogy vállalatunk melyik biztonsági fokozatba tartozik, holott ez alapvetően határozza meg, hogy vállalatunknál milyen védelmi előirásokat kell kialakitani. Nagyon rövid idő állt rendelkezésre ahhoz, hogy a végrehajtási utasitás megjelenésétől 1982. október 31-ig megfelelő alapossággal kidolgozzuk vállalatunk Számitástechnikai Védelmi Szabályzatát.

Nyilvánvaló, a végrehajtási utasitás és a saját szabályzatunk is előirja olyan biztonságtechnikai eszközök beszerzésének a szükségességét, illetve olyan számitástechnikai eljárások megvalósitását, mely pénz- és időigényes.
Ezek biztositását anyagi lehetőségeinkhez mérten fokozatosan tudjuk megvalósitani.
Természetesen figyelmbevéve a feladatok rangsorolásánál mindig a bekövetkezhető kár nagyságának a mértékét.

A védelmi előirások megvalósitását jelentősen elősegiti az, hogy már a korábbi években szabályoztunk olyan területeket, amelyek tüz- és vagyonvédelemhez, az iratkezeléshez, a külföldi kapcsolatok létesitéséhez, a szerződéskötéseink rendjéhez, a számitástechnikai rendszerek dokumentációs, üzemeltetési rendjéhez kapcsolódtak.
Ezek az előirásaink a nem emlitetteken kivüliekkel együtt jól biztositották vállalati politikánknak azt az elemét, amelyre már a bevezetőben is utaltam, vagyis ügyfeleink gyors, pontos határidőre történő, megbizható, korrekt, biztonságos kiszolgálását.

Biztonságos tevékenységünk nagy része ma is jól leszabályo-

zott, ugyanakkor feladatunk, hogy a számitástechnikai rendszerek titok-, vagyon- és tüzvédelméről szóló rendelet, illetve végrehajtási utasitás alapján továbbfejlesztésre kerüljenek. Emellett egyes területeken természetesen uj belső szabályozásokat kell kiadnunk, ezzel is biztositva azt, hogy a tárgyban megjelent rendelet elvárásainak maradéktalanul eleget tehessünk.

Vállalatunknál azt a gyakorlatot kivánjuk követni, hogy vállalati szinten kialakitottuk a Számitástechnikai Védelmi Szabályzatunkat, amelyet benyujtottunk jóváhagyásra felügyeleti szervünknek, de emellett a 17 számitóközpontnál is kidolgozásra kerül a számitóközponti Számitástechnikai Védelmi Szabályzat, amely elsősorban a helyi sajátosságok figyelembevételével, a vállalati előirások alapján szabályozza az adott számitóközpont számitástechnikai védelmi rendjét.

Vállalati szinten függetlenitett adatvédelmi felelős szervezi és irányitja, továbbá ellenőrzi ezen tevékenységünket, mig az egyes gazdálkodó egységeinknél az adatvédelmi felelősi feladatkört a számitóközponti igazgatóknak alárendelt társitott munkakörként végzik el munkatársaink.

Az adatvédelmi felelősi rendszer szervezetének kialakitása mellett hangsulyozni kivánom, hogy a védelmi szabályzatok előirása, azok betartatása kiemelt vezetői gyakorlatnak minősül.

A vállalati Számitástechnikai Védelmi Szabályzatban gondoskodunk a számitástechnikai berendezéseink védelméről, a véletlenszerüen bekövetkezhető károk lehetőségeinek minimalizálására. Ennek érdekében eddigi gyakorlatunknak megfelelően kiemelt gondossággal látjuk el berendezéseink rendszeres karban-

tartását, kialakitottuk a bekövetkezett katasztrófák esetén az áttelepitési tervet, kijelöltük az egyes számitóközpontok háttér számitóközpontját.
Bár megemlitem, hogy hálózatunkra mindig jellemző volt a gazdálkodó egységeink közötti jó együttmüködés, egymás kisegitése és ez kellő biztonságot is jelentett felhasználóink számára, mert üzemzavaraink estén a társszámitóközpont kapacitásán a szerződésben vállalt határidő betartásával teljesiteni tudtuk kötelezettségeinket.

Védelmi szabályzatunkban meghatároztuk a számitástechnikai munkafolyamatokra vonatkozó előirásokat, külön a számitástechnikai rendszerek készitésére vonatkozóan. Itt kitértünk a szerződéskötéskötéseknél alkalmazandó védelemmel kapcsolatos előirások meghatározására, ügyfeleink részéről az adatok minősitésére és azokkal kapcsolatos védelmi előirások irásos dokumentálására.
Meghatároztuk az üzemeltetéssel kapcsolatos védelmi előirásokat, a mágneses adathordozók tárolásának és kezelésének rendjét, a több példányban készitendő másolatok biztonságos megőrzésének formáját, amely a felhasználó igényétől függően történhet részben a számitóközpontnál, részben pedig a megrendelőnél is.

A kijelölt együttmüködő számitóközpontok kölcsönösen, egymást segitve kell hogy gondoskodjanak az alapsoftware termékek és az alkalmazói felhasználó programcsomagok megőrzésének formájáról.
Külön szabályoztuk a TAF környezetben alkalmazandó védelem gyakorlatát.

Kiemelt hangsulyt kap szabályzatunkban a természetes és a jogi személyekre vonatkozó védelmi előirások rendszere. Ez felveti, hogy számitóközpontjainkban csak megbizható, jól

felkészült személyek dolgozhassanak, sajnos itt hangsulyoznom kell, hogy ezt jelenleg bérezési lehetőségeink, több müszakban történő üzemeltetésünk nagyban neheziti
Az adatrögzités területén is olyan megbizható személyekkel kell dolgozni, akik tudatában vannak annak, hogy olyan munkafolyamatban vesznek részt, amelyben a feldolgozásra kerülő adatok állami, üzemi vagy személyre szóló titoknak minősülhetnek és azok védelmét állami törvényeink is garantálják.

Ma ezt a területet kicsit kérdésesnek tartom, hiszen az ezen a területen dolgozó munkatársaknál nem válogathatunk a jelentkezők tömegében.

Végül vállalati védelmi szabályzatunkban főbb vonalaiban meghatároztuk az adatvédelmi felelős feladatkörét, a funkciójához kapcsolódó jogait és kötelességeit.

Gondoskodunk szabályzatunkban a Számitástechnikai Védelmi Szabályzat belső oktatásának rendjéről is.

Korreferátumomban röviden utalni kivántam körülményeinkre,az ezek között kialakitott védelmi szabályzatunk jelentősebb előirásaira.
Tudatában vagyunk annak, hogy az adatvédelemre kiadott rendelet és végrehajtási utasitás egy folyamatot indit el, egy olyan folyamatot, amelyet bizonyos mértékig még megjelenése előtt is a számitástechnikai vállalatok saját területükön több kevesebb sikerrel szabályoztak.

Ma az előirások alapján ismerjük az alapkövetelményeket, amelyekhez igazodnunk kell,de tudatában kell lennünk annak is, hogy a jövő gyakorlat felvet olyan területeket, amelyeket ujonnan, vagy ismételten szabályozni kell. Ezért a kia-

lakitott védelmi szabályzatunknak a gyakorlatban érvényt kell szerezni, gondoskodni kell karbantartásáról, valamint továbbfejlesztéséről.

Ennek szellemében vállalatunk kapcsolatot alakitott ki a SZÁMALK adatbiztonsággal foglalkozó szakembereivel. Megállapodtunk egy adatvédelmi, adatbiztonsági ellenőrzési mintarendszer kidolgozására irányuló kutatási, fejlesztési együttmüködés létrehozására. Terveink szerint a közös munka eredményeképpen a létrehozott mintarendszer egy OTP feldolgozás vonatkozásában kerülne kidolgozásra, amely kritikusan megvizsgálná eddigi gyakorlatunkat, a szerzett tapasztalatok alapján meghatározná a számitástechnikai folyamataink feldolgozására vonatkozó biztonságos előirások feltételeinek szükségességét.

A közeli években még a számitástechnikai kultura elterjesztése volt egyik kiemelt feladatunk, melyben vidéki hálózataink létesitésével a SZÜV is jelentősen kivette a részét, ma az adatfeldolgozó rendszerek biztonsága a számitástechnika önálló szakterületévé fejlődött.

Vállalatunknál szeretnénk ezt a szakmát jól elsajátitani, gyakorlatban jól hasznositani, mert ez az üzemeltetőnek és a felhasználónak egyaránt alapvető érdeke és ehhez megfelelő alapot jelent a számitástechnikai rendszerek titok-, vagyon- és tüzvédelmére megjelent BM rendelet, valamint a kiadott végrehajtási utasitás.

dr. Hermán János:

AZ ADATVÉDELEM IPARVÁLLALATI TAPASZTALATAI
/KORREFERÁTUM/

Mindenekelőtt szeretném kiemelni, hogy a CHINOIN-ból jöttem, és amiről beszámolok, az elsősorban a mi vállalatunkra vonatkozik.
Nincs felhatalmazásom, hogy más iparvállalatok nevében korreferáljak, de azt hiszem a mi helyzetünk adatvédelem szempontjából sok más iparvállalatéhoz hasonló, azonos problémákkal küszködünk.

Néhány szóban milyen is ez a mi "helyzetünk".
Aki a HÉT cimü TV müsor előző két heti adását figyelte, annak számára kiderült, hogy a gyógyszeripar részben a világgazdaságban tapasztalható recessziós hullám, részben egyéb okok miatt nem most éli fénykorát.

Miért mondom ezt az adatvédelmi konferencián?
A közmondás ismert. "Az idő pénz" a biztonság nyelvére átforditva ez még inkább igaz - a biztonság nagyon sok pénz.
Ott ahol a termékszerkezet váltás, exportbővités stb. a jelszó, a számitástechnikusok csendesebbek kell, hogy legyenek, igényeiket redukálniuk kell, bármennyire is indokoltak legyenek.

Szerencsére vannak az adatvédelemnek olyan területei is, melyek nem igényelnek beruházást és itt csak tényleg rajtunk mulik mit érünk el.

Engedjék meg, hadd szóljak néhány szót számitástechnikai hátterünkről, alkalmazásainkról, mely egyrészt megvilágitja miért kell az idevonatkozó állami rendeleteken tulmenően fog-

lalkoznunk az adatvédelemmel, másrészt megadja e munka hátterét.

A CHINOIN-ban 1968 óta müködnek számitástechnikai rendszerek és 1976 óta már a bérmunkát az önálló számitóközpont váltotta fel.
A számitóközpont fizikai biztonság szempontjából jól felszerelt, tüz és füstjelző berendezések, megfelelő oltóeszközök stb. beszerzésére,karbantartására az üzem vegyi jellegéből adódó tüzveszélyesség miatt mindig is nagy sulyt helyeztek.
A klimatizáció a géppark üzembiztos müködését, a mágneses adathordozók megfelelő tárolását elősegiti.
Helyileg a számitóközpont a vállalat más részlegeitől viszonylag elszerparáltan müködik, igy a számitóközpont fizikai védelme külső illetéktelen behatolások ellen jól biztositható.

Nem ilyen egyértelmü a helyzet a számitóközpont területén kivül. Terminál jaink vannak a gyár különböző pontjain és egyre több az önálló kisgép, és a mágneses adathordozók biztonsági másolatai sem olyan körülmények között vannak, mint ami a számitóközpontra jellemző.

A '68-as kezdésből azonban több előny is származik.

- A felhasználók viszonylag magasabb számitástechnikai kulturával rendelkeznek adatvédelmi biztonsági szempontból is.
  Rendszereinkre jellemző, hogy az adatokat a felhasználók viszik be a náluk elhelyezett terminálokon keresztül. Részben szakértelmük, részben programba épitett ellenőrzések által nő a feldolgozások megbizhatósága.
  Az adatrögzitéssel kapcsolatos védelmi problémáink

igy erősen lecsökkentek.

- Olyan üzemeltetési rend alakult ki, mely biztos üzemvitelt tesz lehetővé, szalagok felcserélése, állományok véletlen törlése nem fordul elő.

Ha áttekintem adatvédelmi helyzetünket, a technológiai lánc második, harmadik harmadával, az üzemeltetéssel,felhasználással nincsenek különösebb, vagy megoldhatatlan problémáink.
Operációs rendszerünk ugyan nem biztositja a file-ok teljeskörü védelmét, de ezt a feldolgozások különválasztásával megoldjuk. Problémát inkább a technológiai lánc első fele vagy harmada, a rendszerek fejlesztése, megfelelő minőségü dokumentációja jelent.
Milyen rendszereket fejlesztünk,ezek milyen védelmet kivánnak?

- A gyógyszerkutatásban, molekula tervezésben ma már mindennapos eszköz a számitástechnika. Védenünk kell magát a kutatási eredményeket, az azokat támogató hardware eszközöket /számitógépes mérőeszközök a gyár legkülönbözőbb kutatási helyein megtalálhatók/ és az eredeti software-t.
- A nemzetközileg érvényes előirások szerint számitógépes értékelést kell végezni a forgalombahozandó gyógyszerek toxitológia, farmakológia hatásáról.
- On-line kapcsolatot teremtettünk a Lockheed adatbázis rendszerrel. A tudományos információk védelmén tul, a rendszer üzemeltetésének igen magas deviza költsége is indokolja a hozzáférhetőség szabályozását.
- Termeléstervezéssel, termelésirányitással kapcsolatos számitógépes rendszereink többnyire szolgálati használatra minősitésü információkkal dolgoznak.

- Minőségellenőrzési adatokat tároló és visszakereső számitógépes rendszerünk megbizhatóságát, a nemzetközi előirásokon tul, a gyár jó hirnevének védelme is megkivánja.
- Számviteli rendszerünk teljes egészében számitógépen van, manuális háttér évekkel ezelőtt megszünt és üzembiztonsága a gyár szempontjából kulcskérdés.
- Munkaügyi, bérszámfejtési rendszer adataira vonatkozóan biztositanunk kell a személyhez füződő jogok sérthetetlenségét.

Problémát jelent a fenti rendszerek softwarének, dokumentációjának védelme. Az ipar többi területéhez hasonlóan mi is létszámhiánnyal küzdünk és a napi feladatok gyors megoldásai /termelő üzemről van szó/ a dokumentálás rovására megy, ami viszont a rendszerek megbizhatóságát, karbantartási lehetőségét rontja.

Nagy problémát okoz másrészről az adatok tulzott védelme. Igen sok a különböző szinten minősitett információ. Ez a tul szabályozottság természetesen a szabályok megszegésével jár, de ugyanakkor neheziti a napi munkavégzést.

Komoly gondot jelent, hogy a KSH elnökének az SZVSZ irányelveiben leirt utasitásával ellentétben még nem jelent meg az Ipari Minisztérium végrehajtási utasitása.
Természetesen ez nem jelenti azt, hogy várakozó álláspontra helyezkedtünk. Az eddigiekből is kiderül, sokat tettünk az SZVSZ létrehozásában, illetve annak szellemében a fizikai védelemtől kezdve, a software védelmén, a katasztrófa terven, háttérkapacitás biztositásán keresztül sok területen, melyeket még sorolhatnék.

Én azonban a végrehajtási utasitás hiányát szeretném hangsulyozni, mert igy tisztázatlanok olyan kérdések, mint:

AF kinevezés feltételei
besorolása, anyagi elismerése
szignalizációs jogköre

Nem ismertek a felsőbb szervek adatvédelmi, adatbiztonsági feladatai, elvárásai stb.
Ezeknek a tényeknek köszönhető, hogy vállalati SZVSZ-ünk nincs még végleges formájában, nincs adatvédelmi felelősünk se.

Körülbelül ezek voltak azok a problémák, kapcsolatok, melyet adatvédelmünk szervezése, az SZVSZ létrehozása során találkoztunk, szerveztünk.

Idő hiányában nem beszéltem több olyan problémáról, mely nem csak közvetlenül az adatvédelemhez kapcsolódik, de azért komoly problémát jelent, hogy csak egyet-kettőt mondjak: az SZVSZ beépitése a müködési szabályzatokba, hogy annak szerves része legyen, vagy a nehéz beruházási helyzet, melynek szintén számos adatvédelmi vonzata van.

Ságodi István:

A TÁRSADALMI-GAZDASÁGI FOLYAMATOKRA VONATKOZÓ INFORMÁCIÓK VÉDELME

/KORREFERÁTUM/

Ez a szándékoltan általánositó cim egy rövid hozzászólás előtt aránytalannak tünhet. Azt hiszem azonban, hogy az volna aránytalan leegyszerüsitése adatvédelmi gondjainknak, ha csak a szükebb értelemben vett technikai problémákról beszélnénk. Igaz, hogy ezek az államigazgatást szolgáló számitástechnikai rendszereknél együttesen, egymást felerősitve jelentkeznek; van elég gond. A pillanatnyi technikai problémákon tul azonban gondolni kell a közvetlen előttünk álló feladatokkal is, amelyek a szolgáltatásszerü - mondhatnám társadalmi méretü - információellátás igényes megvelósitását szolgálják. Fejlődésünk jelenlegi szakaszában, az adatvédelmi kérdéseket csak ezekkel egybevetve szabad vizsgálni.

A következőkben ennek tükrében vegyünk szemügyre néhány jellegzetes problémát.

Eszközök

Az alkalmazási igényekből, a feladatok jellegéből következően az államigazgatást szolgáló számitástechnikai központok általában nagyértékü, nagyteljesitményü rendszereket üzemeltetnek; legalább is hazai viszonyaink között ezek relative annak számitanak. Ez önmagában elegendő kritérium a kiemelt biztonsági fokozatba soroláshoz.

Ezek a rendszerek egyidejüleg többféle üzemmódban müködnek, széleskörü interaktiv szolgáltatást nyujtanak. Ehhez helyi terminálhálózattal rendelkeznek; esetenként távoli terminálok, adatállomások kapcsolódnak rájuk. Több rendszernél folyamatban van országos hálózat kiépitése; ezek részben már

üzemelnek is. Röviden: a nagymértékü eszközökhöz távadatfeldolgozás járul. Ez utóbbi az adatvédelem egyik legérzékenyebb pontja.

A korszerü technikai eszközök, sokoldalu operációs rendszerek, valamint a barátságosabb ember-gép kapcsolat lehetővé teszik a szélesebbkörü, közvetlen, szolgáltatásjellegü felhasználás kialakulását. A felhasználók számára a rendszereknek szükségszerüen "nyitottabbá" kell válniuk. Ugyanakkor - az adatvédelem szempontjából - a nagyobb nyitottság miatt az eddigieknél korszerübb védelmi eszközökre van szükség.

Az adatháttér

A legszembetünőbb az államigazgatási számitástechnikai rendszerekben tárolt adatok nagy volumene; nemcsak mennyiségben, hanem esetenként tartalmi kiterjedésben is. Az adatvédelem gondja a mennyiségi tényezők miatt is nagy. Mágnesszalag-köteteket kell kezelni ezres nagyságrendben, gondoskodni biztonsági másolatokról, fizikai és logikai nyilvántartásukról stb.

Az adatok nagyobb része "elemi tényadat"; ezek a társadalmi-gazdasági folyamatok valóságos alakulásáról adnak információt, "visszacsatolást" az irányitási rendszer számára. Ezt növelik a belőlük származtatott összesitések, "aggregált adatok" és mutatók. A másik részt becsült, számitott modellezési, tervezési, prognosztikai adatok alkotják.

Az elemzési, modellezési módszerek jelentős része idősorok vizsgálatán alapul. Emiatt a korábbi időszakokra vonatkozó tényadatok sem avulnak el, az "archiv adatállomány" is aktiv marad és mennyisége folyamatosan növekszik.

Az adatháttérnek az információellátást kell szolgálnia, de

ekkora adatttömegben való tájékozódáshoz már nélkülözhetetlen egy megfelelő "méta-információs rendszer": az adott számitástechnikai rendszerben /illetve az egymáshoz kapcsolódó rendszerekben/ elérhető adatok tartalmi, logikai és fizikai nyilvántartása, eszközök a kereséshez, kigyüjtéshez, egyszerübb összesitésekhez.
Ebben az adatháttérben mindenféle minősitési kategóriáju adat előfordulhat: nem-minősitett, hivatali titok, Sz.H. vagy Sz.T. minősitésü. A valóság bonyolult összefüggéseit tükröző, sokrétü adatkapcsolatok miatt nem könnyü a minősitett adatok elhatárolása, a differenciált, szelektiv adatvédelem megvalósitása, a hozzáférések, elérési utak szabályozása; a közvetett információ-visszanyerés kivédése. Ezekre már az információs rendszerek tervezésénél gondolni kell.

Minősitési kérdések

A tényadatok feldolgozásának jellegzetes müvelete az aggregálás /a legkülönbözőbb szempontok szerinti összesitések, kigyüjtések, gyakorisági táblázatok készitése/ és különböző mutatók számitása. Ezek során, az adatok különböző aggregáltsági szintjei között mozogva, dinamikusan megváltozhat minősitési jellegük. Minősitett államányból készülhetnek olyan összesitések, amelyek adatai nyilvános kiadványokban is megtalálhatók; másrészt nem minősitett adatok feldolgozásával - akár melléktermékként is - előállhatnak olyan eredmények, amelyeknél az információk koncentráltsága vagy különböző részterületek összekapcsolásával nyert ujabb információk megváltoztatják minősitésüket. Igen nagy a feldolgozást közvetlenül végző vagy megrendelő felhasználó felelőssége ilyenfajta dinamikus változások követésében.

Ezek és hasonló problémák különböző módon és mértékben jelentkeznek a különböző számitástechnikai rendszereknél. A kö

zös gond abból ered, hogy igen nagymértékü az adatáramlás az államigazgatás társintézményei között. A formális szabályozások szükségszerü összehangolásán tul /pl. mágnesszalagos adatcsere/, különleges problémát jelent a minősitési elvek, de főként a gyakorlat egyeztetése. Gyakori az elsődleges adatforrásnak számitó intézményeknél a magukat "tulbiztositó" minősités, ami azután a kérdéses adatállományt további utján megmásithatatlanul követi, a hozzátartozó fokozottabb védelemmel, többlet-adminisztrációval együtt. Előfordulhat, hogy egy nagyméretü adatállomány azért számit minősitettnek, mert tételei között egy ezreléknyi minősitett. Ilyen esetekre szükség volna a differenciált minősités gyakorlatának kialakitására.

Az információellátás

Az információ küoönleges érték, az irányitási rendszer hatékonyságához, a döntéselőkészitők, döntéshozók munkájához nélkülözhetetlen. Nagy érték, de csak akkor, ha időben odakerül, ahol szükség van rá. Az információellátás széleskörü szolgáltatás-jellegéről igazán akkor beszélhetünk, ha a technikai /hardware és software/ eszközök, valamint a jól szervezett környezet lehetővé teszik, hogy a nem számitástechnikai képzettségü szakemberek is közvetlenül, "közvetitők" nélkül férhessenek hozzá az adatháttérhez; ha megszokott munkaeszközként használhatják az adatfeldolgozás rutin-eszközeit a számukra éppen szükséges információk elérésére vagy előállitására. Ennek alapfeltétele az adatháttérben való könnyü tájékozódás, az információkhoz való gyors, azonnali hozzáférés - minél kevesebb kötöttséggel, lehetőleg bürökratikus többleteljárások nélkül.

Ezzel együtt a számitástechnikai rendszert is biztonságosabbá kell tenni, hogy a felhasználók kellő jártasság hiányában

ne okozhassanak kárt a rendszerben, de saját adataikban se

Felkészültségünk

Végül arról is szólni kell, hogyan állunk, felkészültünk-e rendelkezésre álló eszközeink elégségesek-e, megfelelőek-e számitástechnikai rendszereink átfogó, következetes, biztonságos védelmére.

Erre csak felemás válasz adható. Egyrészt nem arról van szó hogy mindent elölről kellene kezdeni. Eddig is igyekeztünk szabályozottan dolgozni, az államigazgatás társintézményei között a szabályozásokat összehangolni. A BM rendelet érdeme hogy hangsulyozza az intézkedések átfogó jellegét és rákény szerit a teendők következetes végiggondolására. Ha ezt megtettük, nem lehetünk optimisták.

Először is szembe kell néznük azzal a ténnyel, hogy a korszerü védelemért komoly árat kell fizetni. A fizetség jelen tősen csökkentheti a feladatokhoz mérten nem is olyan nagy rendszerek teljesitményét és kapacitását. Csökkentheti, ha elvégeztük a fokozott védelemhez szükséges eszközök tervezé si, kivitelezési, fejlesztési munkáit és bevezettük őket. E szellemi kapacitásban sem alacsony igény; beruházásokban sem.

Természetesen nem törődhetünk bele, hogy jelenleg nem rendelkezünk korszerü védelmi eszközökkel; ha fokozatosan is, előbbre kell lépnünk. Csak egyet ne tegyünk: azt, hogy adminisztrativ eszközökkel gátoljuk a számitástechnikai szolgáltatások bővülését.

Román Ferenc:

AZ ÁLLAMIGAZGATÁS SZÁMITÁSTECHNIKAI BÁZISÁNAK ADATVÉDELMI TAPASZTALATAIRÓL

/KORREFERÁTUM/

Referátumom célja azoknak az adatvédelmi tapasztalatoknak az ismertetése, amelyekre az Államigazgatási Számitógépes Szolgálat eszközbázisán a különféle nagy államigazgatási rendszerek /pl. népesség-, ingatlan-, egészségügyi-, stb. nyilvántartások/ létrehozásánál. ill. üzemeltetésénél szert tettünk.

Az adatvédelem- és biztonság az intézetünk megalkulása óta napi szintü feladataink közé tartozik. A számitástechnikai védelmi rendelet megjelenése ezért nem ért bennünket felkészületlenül, valójában az ilyen irányu tevékenységeinket szabályozott mederbe terelte. E téma tárgyalásánál az ÁSzSz két lényegi és egymással komoly konfliktusban álló sajátosságából kell, ill. kellett kiindulnunk, nevezetesen

- az államigazgatási alapnyilvántartásoknál társadalmi, gazdasági és politikai jelentőségüknél fogva az adatvédelem és biztonság szerepe kiemelt fontosságu és ennek olyan feltételek mellett kell eleget tenni, hogy
- ezeknek a feldolgozásoknak az üzemeltetése nem kizárólagos használatu számitógépen történik, hanem egy kollektiv számitóközpontban, multiprogramozott környezetben, a távadatfeldolgozás adta lehetőségek felhasználásával.

Mik is jellemzik ezeket a nagy rendszereket?

1./ Népgazdasági fontosságukat kiemeli, hogy létrejöttünket kormány szintü határozatok irják elő.

2./ Mindegyik autonom rendszerként az egységes népgazdasági

információs rendszer részét képezi és igy az állományokhoz jórészt konkurrens hozzáférést kell biztositani.

3./ Rendkivül nagyvolumenü adathalmaz forgalmazása, feldolgozása. Itt jegyezném meg, hogy az adatvédelmi problémáknál mindig felvetődik a védelem szintje és a szükséges költségráforditások közötti lineáris, esetleg exponenciális összefüggés. Az ekkora nagyságrendü adattömegeknél viszont megfelelő szervezéssel, eszközökkel ezek a ráforditások jórészt megtérülhetnek a megtakaritott hibás futtatások, ujrafuttatások vagy mentések által.

4./ Az elsődleges információhordozók többnyire decentrálisan keletkeznek, feldolgozásuk viszont főleg centralizáltan történik. Az információhordozók szállitása fokozott adatvédelmi követelményeket támaszt.

5./ A tárolt adatok okirat jellegüek, ezért az adatok jóságához nagy érdekek füződnek.

6./ A személyekről tárolt, ill. feldolgozott adatokhoz való hozzáférés csak a jogszabályokban rögzitett módon történhet. Ilyen értelemben az adatvédelmi előirásokat a teljes számitástechnikai technológiai láncra kell érvényesiteni.

Ennél a pontnál adatvédelmi aspektusból külön ki kell emelni mindazon személyek döntő fontosságát, akik valamilyen formában a minősitett adatokkal kapcsolatba kerülhetnek, tehát egy számitástechnikai intézetben gyakorlatilag mindenki beletartozik az adatvédelem hatáskörébe. Ezért is alapkövetelmény munkatársainknál az erkölcsi bizonyitvány megléte, ami persze nem csökkenti a különböző ellenőrzési és védelmi intézkedések fontosságát.

Az ÁSzSz-ben jelenleg üzemelő nagy rendszerek legtöbbje a felhasználók saját szervező és programozó apparátusa által készült, bár az elmult években ilyen vonatkozásban is egyre nagyobb részt vállaltunk ezen munkákban. Erre való tekintettel elsősorban azokat a közérdeklődésre számottartó tapasztalatainkat szeretném röviden ismertetni, amelyek a számitástechnikai eszközeink - 2 db nagyteljesitményü CII-HwB számitógép egész országra kiterjedő távadatátviteli hálózattal - üzemeltetése és fejlesztése során halmozódtak fel. Természetesen ezek mind közvetve vagy közvetlenül visszahatnak a technológia többi /szervezési, programozási stb./ területeire is.

Az információrendszerek adatbiztonságának fogalomkörén belül alapvetően két kategóriát kell megkülönböztetni:

- a fizikai adatbiztonságot és
- a logikai adatbiztonságot.

A fizikai adatbiztonság a logikai adatbiztonság előfeltételét és egyuttal az elektronikus adatfeldolgozásban felhasznált eszközök megbizható müködését jelenti. A logikai alatt pedig a feldolgozások produktumának megbizhatóságát, ill. biztonságát értem. Ezen kategóriák elemei közül elsősorban azokat emelem ki, amelyek ma még nem tekinthetők minden számitóközpontban alapértelmezésnek, de esetleg saját fejlesztési munkával másutt is elérhetővé válhatnak.

Meg kell állapitanom, hogy a rendszerfejlesztők körében a gyakorlatban az adatvédelem tervezése szinte teljesen leszükül a logikai szintre. A fizikai védelmi lehetőségek mérlegelésére általában csak valamilyen bekövetkezett negativ esemény kapcsán kerül sor. A két védelmi szint valójában egymás komplemensét kell, hogy képezze.

Az ismertetésre kerülő eszközök és módszerek lényeges tulajdonsága, hogy ezek már megvannak, külön fejlesztésre, beruházásra nincs szükség és alkalmazásuk ma már mindennapos gyakorlat.

Tekintsük át először a mágnes adathordozók védelmét.
A védelem célja az adathordozók fizikai sérülésének elkerülése, a tárolt adatok megsemmisülésének vagy torzulásának megelőzése, az illetéktelen hozzáférés megakadályozása.
Az államigazgatási rendszerek adataikat több ezres, ill. tizezres nagyságrendü mágnesszalag állományon tárolják.

Tapasztalataink szerint a legtöbb problémát azok a mágnesszalagok okozzák, amelyek gyakran vannak szállitásnak kitéve. Ezeknél a fokozott sérülésveszély mellett nem mindig biztositható a feldolgozás előtti megfelelő időtartamu klimatizáció,ami szalagolvasási hibák forrása lehet.

A szolgáltatásképp nyujtott saját gépkocsis expediálásnál jól bevált a zárható müanyag konténer használata, ami egyben az adminisztárciót is csökkentette.

A preventiv módszerek közül az egyik leghatásosabb annak a real time programnak a használata, amely a teljes üzemidő alatt folyamatosan ellenőrzi és feljegyzi az adathordozók azon irás-olvasás hibáit, amelyek többszöri ujrairási, ill. olvasási kisérlettel megszünnék ugyan és igy kivülről nem érzékelhetők, de mindenképpen az adathordozó közeli meghibásodására utalnak. Ezek figyelése és a megfelelő adathordozók forgalomból való kivonása napi szintü feladat az ÁSzSz-ben.

Pár évvel ezelőtt még gyakran hiusultak meg feldolgozások lemezhibák miatt. Ezen ugy sikerült urrá lennünk, hogy megfele-

lő vizsgálatok után szükitettük a gépeinken használható lemeztipusok számát és rendszeres időközönként a lemezeket ujrainicializáljuk, formátumozzuk, kijelöljük az alternate track-eket.

HwB gépeink korszerü operációs rendszere /GCOS/ egyidejüleg támogat különböző lokális és távadat-feldolgozási módokat /helyi és távoli kötegelt, interaktiv feldolgozás, temesharing system stb./ és a multiprogramozás magas szintjét teszi lehetővé. Fontos tulajdonsága a rendszernek, hogy a felhasználók file-jai és katalógusai bármelyik feldolgozási módból és alrendszerből egyaránt és azonos feltételekkel érhetők el. Ez a hozzáférési és kiszolgálási kényelem csak az adatvédelem magas szintjén biztositható.

A katalógusokban és file-okban tárolt adatok védelmét különböző fejlett hardware és software eszközök látják el. Természetesen az adat-kategóriába beleértem a felhasználói programokat is, hiszen valamely program feladata és müködése az adatokéhoz hasonló védelmet követel. Sok esetben, különösképpen az államigazgatás jellegü feldolgozásoknál maga a program az adatok egyedüli kulcsa, ezért a program védelme az adatok védelmének eszközét is jelentheti.

Ezekhez az ugynevezett elsődleges információkhoz hasonlóan teljes körü védelmet kell biztositani a másodlagos információk számára is, amely alatt a hozzáférési jogosultság szabályozására szolgáló adatokat - felhasználói azonositókat, katalógus és file neveket, jelszavakat - értjük.

A védelmi lehetőségek egy része a hardware- és software rendszer integráns részét képezi, mig a többi használata opcionális, tehát az üzemeltető személyzet hatáskörébe tartozik.

Az adatok védelmének hardware eszközei közül kettőt emelek ki:

- a memóriavédelmet és
- az utasitásvédelmet.

A memóriavédelemnél különbséget kell tennünk az operativ tárban előforduló véletlenszerü bithibák és az illetéktelen hozzáférésből adódó adatmeghibásodás között. Az előbbire tökéletes védelmet nyujt a memória automatikus hibajelző és javitó hardware, mely jelzi a bithibákat és 1 bit hibát javit is. Az utóbbi elleni védelmet a HwB gépeken a hardware speciális bázisregiszter segitségével végzi, mely biztositja, hogy az utasitások cime az adott programhoz rendelt memóriaterületen ne mutathasson tul. A program abortja esetén a felhasználói dump is csak az adott felhasználói területről készülhet. Lehetőség van arra, hogy a program befejezése után az adott memóriarész fizikailag is törlésre kerüljön. Erre a felhasználó job-control szinten utasithatja a számitógépet.

Ugyancsak hardware védelem alatt állnak bizonyos gépi utasitások, amelyek lehetővé teszik a memóriahatárok és más határok átlépését. Ezek az utasitások csak priviligizált módban hajthatók végre, melyre való jogosultságot viszont több szinten is ellenőrizzük /JCL, operátor, különlege igény/.

Az adatvédelem software eszközei mind a védett információkat mind a védelem formáját tekintve igen széles körüek.

Az adatállományok és bizonyos rendszerfunkciók hozzáférésének szabályozásában kiemelt és egyben kritikus szerepe van a jogosultság ellenőrzését szolgáló, jelszóval védett felhasználói azonositóknak /USERID-ek/. Nem elsősorban adatbiztonsági /titkossági/ kérdés a munkaszám jogosultság /IDENT/ el-

lenőrzése, hiszen ennek illetéktelen felhasználása rendszerint csak kisebb anyagi károkat okozhat a felhasználóknak, ill. a számitóközpontnak. Ha azonban a géphezférést nemcsak érvényes felhasználói azonositó, hanem érvényes munkaszám megadásához is kötjük, ez tovább csökkentheti az illetéktelen hozzáférés esélyeit. Számitógépeinket mindkét azonositót jelszó védi. Elsőrendü feladatunknak tekintjük az IDENT-ek és USERID-ek védelmére szolgáló jelszók őrzését és védelmét. A jelszavakat az arra jogosult tulajdonosok bármikor megváltoztathatják. A gyakori változtatás fokozza a biztonságot, hiszen a hosszu időn keresztül állandó jelszavak esetében fokozott az információ illetéktelen személyek általi megismerésének veszélye. A gyakori változtatás egyetlen hátránya, hogy nem ritka eset, hogy a felhasználó a saját jelszavát elfelejti. Ilyenkor ezt az információt megfelelő ellenőrzések után csak a megbizó által kijelölt személyek számára szolgáltatjuk ki.

A felhasználói azonositó és munkaszám ellenőrző rendszerünk a job vezérlő utasitás sorozatban elhelyezett felhasználói munkaszámot és jelszavát egy háttértárolón levő nyilvántartás érvényes adataival hasonlitja össze. Ha a keresés sikertelen, a jobot a rendszer törli.

Jelszóval védett katalógusok és adatállományok felhasználásához a jelszót mindig meg kell adni - ezek a listákon viszont nem jelennek meg. A jelszavak érvényességét a nap egyes, meghatározott időszakaihoz is lehet kötni - ezzel az adatállományok használatát időben is korlátozni lehet. A file-ok és katalógusok használatára más felhasználó is kaphat engedélyt, a felhasználás módjának körét azonban le lehet szükiteni bizonyos tipusra, pl. olvasásra, végrehajtásra /program file-oknál/ stb. Az engedélyezetteken kivüli file müveleteket a rendszer visszautasitja.

Mód van a fontosnak itélt file-ok ugynevezett "auditing"-gel való figyelésére is, azaz annak ellenőrzésére, hogy nem kisérli-e meg valaki illetéktelenül a hozzáférést. Minden egyes sikertelen próbálkozásról a rendszerben feljegyzés készül rögzitve azt is, hogy mely azonositó alól kezdeményezték az illetéktelen hozzáférést.

Adatbiztonsági szempontból kivánatos lenne a többszintes katalógusrendszer használata, de kényelmi okokból /hosszu file azonositó stringek megadása a vezérkártyákon vagy a TSS-ben/ felhasználóink nagy része ma még lemond erről.

Szeretném kihangsulyozni azt a negativ tapasztalatunkat, hogy az adatvédelmi módszerek megválasztásánál a kényelmi szempontok időnként az elfogadhatónál nagyobb sullyal esnek latba.

Hosszu időn keresztül a mágnesszalagos adatállományok képezték a biztonsági rendszerünk leggyengébb láncszemét, hiszen fizikai input/output kezelés esetén még cimke ellenőrzés sem volt. Ezt felismerve, kidolgoztunk egy mágnesszalagnyilvántartási és biztonsági rendszert. A rendszer lényege az, hogy minden szalagcimke, illetve mágnesszalagos file hozzárendelődik a tulajdonosának, illetve létrehozójának azonositójához és alapértelmezésben csak ő használhatja. Természetesen ezek az állományok is jelszóval védhetők, továbbá különféle, más felhasználóra vonatkozó engedélyek rendelhetők hozzájuk. Igy szinte teljesen kizárható az illetéktelen hozzáférés vagy a téves használat, felülirás.

Az operációs rendszerünk módot nyujt az adatok kódolással történő titkositására is. Ezt a lehetőséget ma még kevés felhasználó veszi igénybe, bár ez az adathordozók eltulajdonitása és lemásolása ellen is rendkivül hatékony eszköz.

A távadatfeldolgozási környezet elsősorban a kapcsolat felépitésénél és a feldolgozási eredmények remote állomásra való továbbitásánál jelent fokozott adatvédelmi feladatot. A kapcsolatfelépités során a felhasználónak az előbbiekhez hasonló módon azonositania kell magát és természetesen a jelszavakat is meg kell adni. Bármely azonositó hibás megadása a kapcsolat azonnali lebontását eredményezi. A védelmi rendszerünk azt is biztositja, hogy az outptok más felhasználó által nem kérdezhetők le.

Az államigazgatási feladatok speciális igényei miatt nagyon gyakori a nagytömegü outputok mágnesszalagra vitele, majd off-line kiirattatása. Ez egyben lehetőséget ad speciális karakterkészlet, illetve speciális papir használatára is.

Végezetül néhány gondolat a job-szervezési eljárások fontosságáról, amelyek döntően befolyásolják az adatvédelem és a ráforditási költségek arányát. Elég komoly "tanulópénzek" kifizetése után ma már a nagy rendszerek szervezői és üzemeltetői felismerték és alkalmazzák az automatikus job-inditási és a különböző checkpoint-restart lehetőségeket. Nagyon fontosnak tartjuk, hogy az információrendszerek szervezési folyamatában az üzemeltetés szervezése a többivel teljesen egyenszilárdságu láncszem legyen. Tapasztalataink szerint ez a szemlélet a számitástechnikai képzésünkben még nem kap elég hangsulyt.

A rendszerek biztonsága pénzbe kerül és egyben tudomásul kell venni, hogy rontja a számitógépek hatékonyságát is, hiszen pl. az állományok mentése jelentős gépkapacitást köt le ugy, hogy a kimentett állapotokra remélhetőleg sohasem lesz szükség. Tapasztalatok alapján meggyőződésünk, hogy néhány állambiztonságilag fontos feldolgozástól eltekintve, nem a maximális biztonság megteremtését kell célul kitüzni, hanem a cél-

szerüség és a költségtényezők figyelembevételével azokat az eszközöket kell jól kiválasztani vagy megteremteni, amelyek a biztonság és ráforditás közötti optimális kapcsolatot biztositják.

Sajnos meg kell állapitanunk, hogy az előbb emlitett "tanuló-pénzeket" minden nagy rendszer készitésénél külön-külön megfizetik a létrehozók. Ma még nem alakult ki egy egységes adatbiztonsági szemlélet és talán az érdekeltség sem ösztönző olyan irányban, hogy az optimumra törekvés tapasztalatait másutt is hasznositsák.

Remélem, hogy ez a konferencia ilyen értelemben is előrehaladást fog jelenteni.

AZ ADATVÉDELEM MÜSZAKI-TECHNIKAI VONATKOZÁSAI

Strádi Géza:

SZÁMITÓKÖZPONTOK TÜZVÉDELME, OLTÁSI TECHNOLÓGIA

Az elektronikus berendezések - köztük a számitógépek nem tartoznak a kifejezetten tüzveszélyes berendezések közé, tüztől, tüzkártól való megóvásuk mégis fokozott figyelmet, hathatós tüzmegelőző intézkedéseket indokol az ilyen berendezések üzemeltetőitől.
Ezt a különös figyelmet egyrészt ezeknek a berendezéseknek magas anyagi értéke, de talán még ennél is jobban a számitógépben tárolt adatok fontossága vagy a számitógép által vezérelt gyártási folyamat biztonsága indokolja.

Köztudott, hogy egy számitógép - a hozzátartozó adatrögzitő, adattároló, kezelő berendezésekkel fajlagosan nagy értékkoncentrációt képvisel más gépekhez, berendezésekhez viszonyitva. Az ilyen területen keletkezett tüz magától értetődően rövid idő alatt hatalmas tüzkárt eredményezhet. Talán nem is az effektiv tüzkár, tehát a berendezésben keletkezett kár a nagyobb, hanem a termeléskiesés, vagy az egyéb járulékos kár. Gondoljunk csak egy atomerőmüben alkalmazott folyamatvezérlő számitógépben keletkezett tüz kihatásaira.

Természetes, hogy a tüzkárok elkerülésének legbiztosabb módja a megelőzés, ami még a számitógépek elhelyezésének tervezési stádiumában kell, hogy érvényesüljön. Használati szabályok meghatározásakor is érvényesiteni kell azokat a szempontokat, melyek a tüz megelőzését szolgálják.

Magyarországon a BM Tüzoltóság Országos Parancsnokság által kiadott a "Számitóközpontok tüzvédelme" cimü, MI-02-102-79 számu müszaki irányelvek tartalmazza a tervezés, elhelyezés, épités és egyéb tüzvédelmi vonatkozásban az ajánlásokat.

A leggondosabb tervezés, telepités sem nyujthat azonban garanciát a nemkivánatos tüz távoltartására. A számitógép elektromos berendezései, alkatrészei a leggondosabb gyártási ellenőrzés ellenére is lehetnek tüzokozók. Az emberi gondatlanság, felületesség pedig ugyszólván tárháza a tüzkeletkezési okoknak. Ezért mindenképpen indokolt a számitógép védelmére tüzoltó eszközt,tüzoltóberendezést létesiteni.

Következő problémát a témakörben a megfelelő oltóanyag jelenti. Ugyanis a klasszikus tüzoltóanyag,a viz,több vonatkozásban okoz gondot egy elektronikus berendezés tüzének oltásakor. Más oltóanyag használata - pl. az oltópor - szennyező hatása vagy pl. a különböző oltógázok toxikus hatásuk vagy egyéb nemkivánatos kémiai reakciók miatt igényelnek alapos mérlegelést.

Szakemberek körében ma már egyértelmü a vélemény, hogy beépitett, automatikus tüzoltó berendezést kell felszerelni minden számitógépre. Hogy az a berendezés milyen legyen, mivel oltson, ezekben a kérdésekben a tapasztalatok, lehetőségek alapján vannak véleménykülönbségek.

A tüzoltóberendezés és az oltóanyag kiválasztásának indoklására vizsgáljuk meg, hogy milyen jellemző keletkezési, terjedési és kihatásu tüzzel kell számolni számitógépek, számitóközpontok esetében.

Legegyszerübb eset, amit könnyen elintézhetünk, egy,a gépteremben, vagy kiszolgáló helyiségben keletkezett hulladékpapir, irodai berendezés vagy hasonló anyag égéséből keletkező tüz. A kéznél lévő /és legyen kéznél/ tüzoltó készülékkel vagy vödör vizzel kell eloltani.

Természetes a tüz jelzéséről az illetékes tüzoltóság felé ilyen esetben sem szabad megfeledkezni.
Az ilyen jellegü tüzek szennyező, a füstgázok fojtó, toxikus hatásával okozhatnak gondot. Ha sikerül időben eloltani, a drága elektronikus berendezések sértetlenek maradnak.
Bonyolultabb és főleg kihatásaiban veszélyesebb egy elektromos vezetékben, vagy a számitógép alkatrészeiben keletkező tüz. A tüz keletkezhet tulterhelés, helyi tulmelegedés, alkatrészhiba vagy más müszaki okból. A füstölés megindulása után a gép belsejében koromlerakodás kezdődik. Ez a korom megköti az elektromos vezetékek szigetelésére használatos PVC égésekor felszabaduló sósav-gázokat, s kitünő korrodáló központot képez. 1 kg PVC-ből - becslések szerint - a hőbomlás kapcsán annyi sósav képződik, ami elégséges 0,6 kg acél teljes elkorrodálásához, vagy kb. 2 m²-nyi nyomtatott áramköri réz leoldásához elegendő 1 m PVC szigetelés elégetésénél keletkező sósav gőz. Tehát egy egészen kis tüz is okozhat igy nagy kárt. Ezért kell a tüz keletkezését lehetőleg mielőbb észlelni és az oltást folyamatba tenni.

A füst jelenlétének jelzése technikailag megoldott probléma. Erre a célra szolgálnak az un. ionizációs füstérzékelők. Ezeket olyan helyekre kell elhelyezni, ahol a várhatóan keletkező füst mielőbb "megszólaltatja" őket. Fontos szempont, hogy a klimaberendezés ezek hatását ne korlátozza, tehát az érzékelők ne szellőzési irányokban legyenek. Az érzékelők jelzését fény, hang formájában lehet tudatositani és az automatikus oltóberendezések aktivizálására használni. A nálunk is ilyen célra szolgáló automatikus berendezések a füst jelzésekor riasztást végeznek és 20 mp-es késedelemmel inditják az oltóberendezést. A 20 mp alatt a személyzetnek el kell hagyni a helyiséget, hogy az esetleges balesetet elkerüljék.

A számitógépek védelmére kifejlesztett tüzoltó berendezések

- teljes elárasztásos, vagy
- helyi oltást végző

kialakitásban készülnek. Gyakoribb a helyiség teljes elárasztását végző berendezés, ami olyan mennyiségü oltóanyagot - oltógázt - juttat a helyiségbe, hogy ott az égés megszünjön. A helyi oltást végző berendezéseknél a frekventált helyekre irányitott szórófejből áramlik az oltóanyag, s oltja el a tüzet.
Az ilyen tüzoltóberendezések megfelelő védelmet jelentenek, azonban a vakriasztások elkerülése miatt gyakran hatástalanitják az automatikát - mondván, hogy a helyiségben tartózkodnak, várhatóan észlelik majd a tüzet, s bekapcsolják az oltóberendezést. A probléma akkor jelentkezik ha elhagyják a számitóközpontot, s elfelejtik élesiteni a berendezést. Ilyen esetben - és volt már ilyen - a drága berendezés védelem nélkül marad. Másik hibalehetőség, hogyha a tüzjelző megszólalása után nem következik be a klimaberendezés kikapcsolása - amit az automatának kell végrehajtani. Ilyen esetben a klima kiszellőzteti az oltógázt, s a tüzoltás elmarad.

Az elektronikus berendezések tüzeinek oltóanyagai, illetve ezek kiválasztása ugyancsak figyelmet érdemel.
A nálunk használatos automatikus tüzoltó berendezésekben a HALON-1301 nevü oltógázt alkalmazzák. Ez a nyugati importból beszerezhető anyag igen jó tüzoltó képességgel és olyan fizikai-kémiai paraméterekkel rendelkezik, ami ilyen célra különösen alkalmassá teszi, gyorsan keveredik a helyiség levegőjével, s ha mintegy 5 %-os koncentrációt képez, a térben az égés megszünik. A gáz maradék nélkül kiszellőztethető, nem okoz korróziót, az oltási koncentrációban emberre nem veszélyes, mérgezést nem okoz. A gáz elektromosan nem vezető, sürüsége 5,2-szer nagyobb, mint a levegőé.

A helyi oltást végző készülékekhez /és a modern halongázzal oltó kézi tüzoltókészülékekhez is/ a HALON-1211 jelü oltógázt alkalmazzák. Ennek sürüsége a levegőhöz kepest 5,7-szeres. 7 %-os az a koncentráció, ahol tüzoltóképessége már kielégitő. Egyéb tulajdonságai hasonlóak az 1301-hez.

Régebbi berendezésekben - de még napjainkban is készülnek ilyenek - a CO_2 gázt alkalmazták. CO_2 elárasztásos és helyi oltóberendezésekhez is alkalmas, s mivel beszerzése nem jelent import gondokat, számitani lehet kiterjedtebb alkalmazására. A CO_2 nem okoz korróziót, nem hagy nyomot, maradéktalanul elpárolog. Egyik gond az alkalmazásánál, hogy a hatékony tüzoltáshoz a helyiség légterében kb. 53 %-os CO_2 koncentráció az ajánlatos, 5 %-os CO_2 koncentráció viszont már légzési nehézséget, 10 %-os eszméletvesztést, 50 %-os pedig halált okoz néhány percen belül.

Tehát egy halonnal oltó berendezés esetében a veszély viszonylag kicsi a kezelőkre, ugyanakkor CO_2 oltógáz alkalmazásakor csak a jól kiszellőztetett helyiségben szabad légzésvédő készülék nélkül belépni.

Halonnal müködő oltóberendezés esetén még egy veszély fenyeget. Ugyanis 500°C-t meghaladó hőmérsékleten a halonok bizonyos foku bomlása megy végbe, aminek terméke fluorhidrogén, brómhidrogén, klórhidrogén lehet. Ezek csipős szaga figyelmeztet jelenlétükre, s mérgező hatásuk miatt belélegzésük kerülendő.

Összefoglalva megállapitható, hogy a drága elektronikus berendezések tüzvédelme, annak müszaki feltételei a kor technikai szintjén megoldottak. A védelmi berendezések anyagi kihatásai relative nem magasak, annak ellenére sem, hogy az auto-

matikus halonnaloltók nem tartoznak a tömegcikkek közé. Gond, hogy a legmegfelelőbb oltóanyagok jelenleg csak nyugati importból szerezhetők be.

Az elektronikus berendezések tüzvédelmében az ujabb irányzatról is szólok néhány szót.
Néhány évvel ezelőtt az elektronikus berendezések tüzeinek oltására senki sem mert volna vizet készenlétben tartani. A viz, mint elektromos vezető - ugy vélték - beláthatatlan oltási károkat okozhat.
Néhány az USA-ban történt számitógép tüz, illetve számitógép környezetében keletkezett tüz és ezek oltási tapasztalatai a következő tapasztalatokat, s azok nyomán megfontolásokat hoztak felszinre:

- a számitógép - helyiségében gyakran sok sornyomtatópapir van, gyakran tárolnak ott lyukkártyákat
- a lyukszalagokat müanyag tárolókban tartják.

Ezek az anyagok elég könnyen gyulladnak, erős füst-képződéssel égnek, s oltásukra a porlasztott viz a leghatékonyabb.
A halonnal oltás egyik előfeltétele a zárt helyiség, a leállitott klima. Porlasztott vizzel oltás még nyitott ablaknál is hatásos.
Az oltógázok oltóhatása a láncreakció antikataltikus leállitásán alapszik, hütőhatás csekély. A porlasztott viz az intenziv hütőhatással olt, utóégés, parázslás szinte kizárt.

Ellenpóluson: nagy vizkár.

Néhány évvel ezelőtt, ha valaki pl. egy tüzkárt szenvedett elektronikus berendezést vizzel akart volna lemosni, megütközést keltett volna.
Kényszerhelyzet, majd tudatos kisérlet igazolta, hogy a lakkal fedett nyomtatott áramkörökre, elektronikus alkatrészek-

re a viz nincs olyan károsító hatással, mint azt gondolták volna. Lényegesen nagyobb kárt okozott, amikor a számitógépet a tüz után kitakaritották, az égett részt kicserélték, és üzembe helyezték, mintha a gépet vizzel alaposan kimosták volna üzembehelyezés előtt. Egy svéd biztositótársaság kisérletet folytatott egy 360/2020 tipusu IBM számitógépen. A gépet füstnek, hőnek, viznek tették ki. A savas füst a gép meghibásodását idézte elő. Félórán keresztül vizet permeteztek a gépbe, majd ventillátoros hősurgárzóval kiszáritották. Ezt követően a gép 11 héten keresztül müködött kifogástalanul. Eztuán az IBM szakértője megvizsgálta a gépet, s annak árát 10 %-ban elérő javitási költség szükségességét állapitotta meg.

Más amerikai kisérletek is igazolták, hogy a vizes lemosás a legjobb módszer a savas füsttel szennyezett, kormos elektronikus berendezések tisztitására. A NASA egyik ürhajózási távmérő központjában egy alkalommal iszappal és vizzel árasztották el - valami hiba folytán - egy számitógépet, négy nappal egy mühold tervezett felbocsátása előtt. A berendezést gumitömlővel, vizzel kimosták, majd a hősugárzóval kiszáritották. A berendezés kifogástalanul müködött, a müholdat felbocsátották.

A példák is igazolják, hogy a viz nem jelent olyan veszélyt, mint a szigetelő anyagok égése során keletkezett savas füst. Kézenfekvő, hogy akkor a keletkező számitógéptüzek oltására is alkalmazható az olcsó, kedvező tüzoltó tulajdonságokkal rendelkező viz. Amerikában már széles körben terjed a vizzeloltó sprinklerberendezések alkalmazása számitógéptüzek védelmére.

Természetes, számos technikai nehézség a viz ilyen célu alkalmazásával is jelentkezett, de ezek megoldása nem jelentett különösebb gondot. Pl. a számitógép burkolat alatt, árnyékolt részeit csak megfelelő helyre szerelt fuvókával lehet beszórni. Ehhez csővezetékek elhelyezésére vont szükség. Különös gondot kellett forditani a téves müködésnek, mert a nem égő gép locsolása nem kivánatos. Erre olyan biztonsági szeleprendszereket fejlesztettek ki, ami csak tényleges tüz esetén teszi lehetővé a viz áramlását a gépbe. Ez a szeleprendszer ugy müködik, hogy a füstjelző megszólalását követően készenléti állapotot vesz fel a berendezés, ami alatt a vezetékrendszer nyomás alá helyezése, riasztási jelzések leadása értendő. További jelre a szükséges helyen megindul a vizpermetezés. Természetes ez nem az egész gép permetezését jelenti, hanem csak a tüzkeletkezés helyének és közvetlen környezetének locsolását.

A vizzel oltó sprinkler berendezések az elektronikus berendezések esetében olyan további előnnyel járnak, hogy nem kell tartani sem az oltógáz, sem a hőbomlás termékeinek toxicitásától. Nincs szükség olyan elővigyázatossági szabályokra, ami a visszakapcsolás elfelejtésének veszélyét rejti magában.

Egy amerikai statisztikai felmérés szerint 1972-76 között 32 számitógéptermi baleset 56 %-ban volt tüz. A teljes veszteségek 14 %-át tulajdonitották az oltóviznek ezekben az esetekben. A vizzel eloltott tüzesetek többségében néhány órás száritási müvelet után a gépet üzembe lehetett helyezni.

Amerikában már előnyben, Angliában elfogadva, más nyugateurópai országokban terjedőben van a számitógépek tüztől védelmére a vizzeloltó sprinkler berendezés. Nálunk még ujdonságnak számitana, ha ilyent létesitenének. Itt még egyeduralkodó a halonnaloltó.

A CO_2 alkalmazásának is van ujabb változata az elektronius berendezések tüzvédelmében. Francia megoldás szerint nem folyékony CO_2-vel árasztják el a számitógépet, hanem előzetesen expandáltatják azt egy tartályban, majd a gázt vezetik a gépbe. Ezzel el tudják kerülni a folyékony szénsav hirtelen hütőhatását, ami nemkivánatos mellékhatás volt a korábbi rendszerekben, s esetenként az oltási kárt növelte. Az uj rendszer szerint 70 dkg CO_2-t engednek be légköbméterenként a számitógép helyiségbe kb. 1,5 bar nyomáson, s az oltást ezzel végzik. A CO_2 toxikus hatását természetes nem lehet elkerülni.

Ilyen berendezés hazai létesitése még nem került szóba.

Összefoglalva megállapitható, hogy a számitógépek elektronikus berendezések megelőző tüzvédelme, tüzoltási technológiája, oltóanyagai kimunkált, ismert eljárások, hozzáférhető anyagok. Magyarországon az MMG. gyárt és szerel ilyen berendezéseket. Egy svéd minta alapján gyártott és HALON 1301 oltóanyaggal müködő berendezésük rendelekzik a BM TOP egyetértő hozzájárulásával. Több ilyen berendezést szereltek már fel, köztük a Paksi Atomerőmü számitógépeinek védelmére is.
Számos egyéb halonnaloltó berendezés van az országban, ezek közül néhány már müködött is tüzeset kapcsán.
A fejlődés ezen a vonalon várhatóan a vizes sprinkler alkalmazása felé tart, azonban még néhány szerelvény hazai gyártását kell megoldani. A halon nyugati import, ezért a vizes megoldás mindenképp figyelmet érdemel.

Bojti György:

A GELKA VAGYONVÉDELMI SZOLGÁLTATÁSA, SZÁMITÓKÖZPONTOK SPECIÁLIS VÉDELME

A GELKA vagyonvédelmi szolgáltatása nagyon uj. Mintegy két és fél éve foglalkozunk intenzivebben ezzel a profillal. Létrehoztuk országos hálózatunkat, mely központi szakirányitás alapján végzi az egész országban ujszerü munkáját.

Ez az ujszerüség főként abból áll, hogy komplex szolgáltatásként a vagyonvédelem egészét szeretnénk ügyfeleinknek felajánlani és nyujtani. Ennek értelmében vagyonvédelem alatt annak teljes rendszerét értjük:

Védelmi cél szerint: tüz- és betörésjelző rendszereket együttesen.

A szolgáltatás sikjai szerint: igénybejelentéstől a karbantartásig, felujitásig tartó teljes szakaszt, mely átfogja a szaktanácsadást, tervezést, kivitelezést és a teljes szerviz-tevékenységet.

Felkészültünk titkos anyagok kezelésére és ilyen feladatok vállalására. Ezen tevékenységeknek megfelelően célirányosan válogattuk meg és képeztük ki szakembereinket, illetve alakitottuk ki szervezeti felépitésünket és müködésünket. Igy sokoldaluan - müszaki, tüz-, és betöréstechnikai, általános vagyonvédelmi területen egyaránt - kiképzett szakembergárda áll rendelkezésünkre. Ezen kiképzésben és általában az előkészületi szakaszban nagy segitséget kaptunk az illetékes hatóságoktól, és intézményektől /BM, BM-TOP, ÉMI és még sokan/. Többségükkel továbbra is folyamatos a kapcsolattartás, nemcsak tervszerü, állandó kiképzésünk érdekében, hanem a napi, gyakorlati problémák legjobb megoldásáért is.

Szolgáltatásunk minősége vonatkozásában célunk kettős:

- Ügyfeleink igényeit ugy elégitsük ki, hogy az
- illetékes hatóságok és véleményező intézmények vonatkozó előirásainak, illetőleg követelményeinek is eleget tegyünk.

Ez a kettősség a jó munkakapcsolatok részben tervszerü, részben promt, de mindenképpen folyamatos karbantartásában oldódik fel, egyuttal ez biztositja a feladat mindkét irányu, megfelelő minőségü teljesitését is.

Eszközök, gyártók vonatkozásában ha lehet még bonyolultabb a helyzet. Együttmüködésünket minden számottevő - és nagyon sok kisebb - gyártónak felajánlottuk, illetve ezuton is felajánljuk. Ismertettük célunkat és kértük ennek, eszközök gyártásával, illetve fejlesztésével való támogatását. E téren sikereinkről hadd ne beszéljek most, mert tul kevés az eredmény, tul sok a kudarc.

Bizonyos, hogy mi is követtünk el ilyen téren is hibákat. Mégis az eddigi kudarcok alapvető okaként azt a gyártói felfogást tartom, mely szerint "a megrendelő azt vegye, amit gyártok". Kevesen választják a nehezebb, de egyetlen célravezető megoldást: azt gyártani, amit vesznek, illetve vennének.

Ily módon a magyar piac vonatkozásában egyrészt van egy igény, kereslet, másrészt pedig a gyártók kinálata. A kettő nemigen akar összetalálkozni. És ha ez a találkozás mégis megtörténik, ma még a legkevésbé sem perspektivikus és konstruktiv módon, hanem a legegyszerübb formájában az igény ereszkedik le kénytelen-kelletlen a kinálat szintjére. Természetesen sötétebbre sem akarom festeni a helyzetet, mint amilyen. Lassan, de megindultak az uj kezdeményezések és az

is eredmény, hogy lényegében vannak hazai eszközök. De korántsem olyan szinvonaluak és szolgáltatásuak, amilyenek lehetnének, amire az objektiv lehetőségek adottak mind technológia, mind szakismeret vonatkozásában.

A számitóközpontok speciális védelme az általános vagyonvédelmi tevékenységen belül különleges helyet foglal el. Nemcsak a számitóközpont jellegéből fakadó sokoldaluság miatt, hanem üzemvitelének sajátosságaiból adódó különleges védelmi koncepció és védelmi eszköz igénye miatt is. Ez elmondható a tüz és betörés /behatolás/ védelmi területre egyaránt.

A jellegéből fakadó sokoldaluság megnyilvánulásai, mint adat és információ-védelmi szempontok /a teljesség szándéka nélkül/ az alábbiak:

- illetéktelen behatolás, belépés ellenőrzés
- illetéktelen hozzáférés, lekérdezés /software, ill. adat/
- véletlen adatmegsemmisülés - adatmentés
- információ-kisugárzás: parazita sugárzásból visszanyert hasznos információ, adat
- adathordozók védelme eltulajdonitás ellen
- különleges áramlástani körülmények a klimatizációból, illetve a nagyteljesitményü gépek szellőztetéséből következően stb.

Mind megannyi speciális szakterület, kutatási téma. Egyenként önálló előadást érdemlő szakanyag-mennyiséggel.
Az üzemvitel sajátosságaiból adódó szempontok:

- sokszor 24 órás üzem

- felügyelettel, ill. anélkül futó időszakok, vagy szakterületek váltakozása,
- szükség esetén egyes szakterületek külön védelme - belépés-ellenőrzéssel - oda beosztottak számára egyszerü belépés, illetéktelenek kizárásával,
- esemény rekonstruálás - hibaelháritás, vagy felelősség megállapitás miatt stb.

Az előbbiekből látszik, hogy a speciális jelleget - ezen előadásban - csak érinteni van mód az általános ismertetés keretében.

A kockázat és igény viszonyában megállapitható, hogy minél magasabb kockázati szintről van szó - ami a szükséges biztonsági szintet is meghatározza - annál kisebb mennyiségü az igény.
A legnagyobb mennyiségü igény a magánszektorból lakás, családiház, autó stb., a legkevesebb pedig a kormányszintü objektumokból származik. Mig a kockázat az utóbbinál igen magas, az előbbinél viszonylag csekély mértékü /és természetesen más jellegü/.

A vagyonvédelem célja időt nyerni egy vagyon elleni esemény /tüz/ vagy cselekmény /betörés/ minél korábbi fázisban való meghiusitásához.

Annak megvilágitásához, hogy a fenti cél müszakilag mely főbb paraméterekkel, milyen ellentmondásos egységben valósitható meg, a szabotázsvédelem, szabotázsbiztonság fogalmával is meg kell ismerkednünk.
A szabotázsvédelem - eltekintve a legegyszerübb riasztókészülékektől - minden, minimálisan közepes szintü igényt kielégitő vagyonvédelmi rendszernél előforduló alapkategória. A

fogalom lényegében azt jelenti, hogy a teljes rendszer, illetve annak minden eleme ugy van kialakitva, hogy önmagát folyamatosan felügyeli és védi illetéktelen beavatkozás, hatástalanitási kisérlet /pl. érzékelők megrongálása, vezeték elszakitása, központ felnyitása stb./ ellen. Ha ilyen kisérlet bekövetkezik, azonnal - üzemmódtól függetlenül - szabotázsjelzést ad, melynek végleges megszüntetését csak a szakszerviz tudja végrehajtani a szabotázs jelzést kiváltó ok megkeresése és megszüntetése után. A szabotázs-biztonság az elektronikának az ilyen jellegü cselekmény észlelésére való érzékenységét jelenti.

A fentiek után már értelmezni tudjuk a kölcsönös ellentmondásokat a vakriasztás-érzékenység, szabotázsbiztonság és megszólalási biztonság között. Minden készülék gyártásakor, érzékenységének és hatósugarának beállitásakor, a rendszertervezéskor és felépitéskor, a rendszer beüzemelésekor a szakembereknek erre a háromszögre tekintettel kell lenni, ahhoz, hogy megfelelő szintü szolgáltatást nyujtsanak.

Egy általános vagyonvédelmi rendszer elvi felépitését, annak komplexitását szemlélteti védelmi cél szerinti bontásban a rendszertechnikai felépitésen végighaladva az alábbi séma:

Érzékelők:
- müködés szerint:
  - passziv
  - aktiv
- védelem szerint:
  - elmozdulás - tárgyvédelem
  - felületvédelem
  - térvédelem

Jelzésadók: cél: emberi beavatkozás /jelzés/
- kézi
- láb

Vezérlők:

cél: a központ üzemmódjának vagy egy-egy védett terület állapotának a megváltoztatása
- illetéktelen személy általi kezelés kizárása

belsők:
- kapcsolók! csak a rejtés marad
- kulcskapcsolók
- kódkapcsolók

kezelő tablók

külsők:
- kulcskapcsolók
- blokkzárak /csoportzárak/
- kódkapcsolók

Központok:

cél: az érzékelők és jelzők, illetve vezérlők által adott jelek fogadása, kiértékelése és az előre meghatározott program, vagy beállitás szerinti intézkedés /reagálás, jelzés/ végrehajtása,
- ide sorolhatók a központnak nem nevezhető kisriasztók is!

Jelzővonalszám szerint:

- kis riasztóközpontok: 4 jelzővonalig
- közepes " : 4-8-10 jelzővonalig
- nagy " : 10 jelzővonal felett

Védelem- és riasztás-szervezés szerint:

- egyszerü
- közepes
- bonyolult szervezésü

Jelzővonal:

A központ 1-1 jelzőcsoport jelzéseit fogadó és kiértékelő elektronikus egysége

Fajtái: /csak a korszerűbb központok rendelkeznek jelzővonal programozási lehetőséggel, tehát csak itt lehet többféle jelzővonalat megkülönböztetni./

A jelzővonalak a rendszer N állapotában különböznek funkciójukkal egymástól, É állapotban mind külső riasztást ad.

N=nappali; É=éjszakai

Jelzővonal	N	Megjegyzés	É
szabotázs	belső riasztás	kivülről nem törölhető	külső riasztás
támadás	külső riasztás	nem kapcsolható le	
betörés	belső riasztás		
lopás	fényjelzés		
B/L	belső/külső riasztás	átkapcsolástól fg.	

Jelzők:

A riasztás hang, vagy fényjelzését megjelenitő eszközök - hangjelző
- fényjelző
- hang- fényjelző

Az előzőekben ismertetett általános védelmi rendszert a védelmi koncepció teszi speciálissá, az adott objektumra jellemzővé.

Jól érzékelhető, hogy ez a folyamat kezdettől komoly együttmüködést igényel és feltételez a megrendelő és a szakember

között. Sőt, hogy - a lényegében közösen kialakitott - védelmi koncepció maradéktalanul megvalósulhasson, a vagyonvédelmi szakember adatszolgáltatása után a megrendelőnek magának is intézkedéseket kell foganatositania az őrzési rendszer és a beavatkozás megszervezése érdekében. A megfelelő védelmi koncepcióhoz az alábbi kérdés-sor megválaszolásán keresztül vezet az ut:

1. Mit kell védeni?
2. Mi, illetve ki ellen?
3. Mekkora az érték?
4. Hol található az objektum?
5. Milyen a környezet?
6. Milyen a mechanikus védelem?
7. Milyen a szervezet?
8. Ki a beavatkozó? /intézkedő/
9. Milyen előirásokat kell betartani?
10. Fedezet? Ügyfél pénztárcája?
11. Ki a döntésre jogosult személy?

Hogyan néz ki ez egy számitóközpont esetében?

1. Mit?: - eredeti szalagok, lemezek és
   - másolatok
   - hardware
   - áram, viz, szellőzés, telefonkábel

2. Mi, illetve ki ellen?:
   - müszaki hiba
   - tüz
   - illetéktelen személy /betörés, lopás, támadás, szabotázs, információszerzés

3. Mekkora érték?:
   - gépeké /hardware/ meghatározható
   - adatoké, többnyire pénzben nem kifejezhető, esz-

mei, erkölcsi érték /vagy éppen ipari, vagy államtitok/

4. Hol?:
   - helyszin- és épitészeti rajz szerint /gépterem, terminál, adattár stb./

5. Környezet?:
   - utca /forgalom, fekvés stb./
   - földszint

6. Mechanikus védelem?:
   - keritès
   - rács az ablakon
   - zár stb.

7. Szervezet?:
   - vezetés, programozók, rendszerszervezők, karbantartó- és üzemeltető müszerészek, portás, takarító személyzet stb.

8. Beavatkozó:
   - portás, megbizott őr
   - rendőrség, tüzoltóság

9. Előirások?:
   - klimaberendezés müködése, tüz esetén beavatkozás
   - BM-TOP előirások
   - helyi sajátosságok

10. Fedezet?:
   - beruzázásra keret nincs!
   - tüzjelző központ ára nagyobb mint 20.000,- Ft
   - 20.000,- Ft felett beruházás!

11. Döntésre jogosult személy?
   A 10 pont ellentmondása miatt eddig még nem találtuk meg!

Igy a védelmi koncepció:

- védendő: személyek, adatok, berendezések
- hol: gépterem és kisegitő helyiségek
- szabotázs, lopás, betörés és támadás ellen
- riasztás: külső és belső hang- és fény, illetve rendőrség és tüzoltóság távjelzéssel
- kezelés: - a bejárat nappal belépésellenőrzéssel
  - kódkapcsoló /vezérlő/ a riasztás-szervezés átkapcsolására /éjjeli- és nappali szervezés/
- szervezés: - vezetőség
  - számitóközpont személyzete
  - takaritó személyzet
  - szerviz személyzet

A védelmi koncepcióra alapozva az épület és szervezet sajátosságainak figyelembe vételével megkezdődhet a tervezés.

A tervdokumentáció készitésének megkezdése előtt tervbirálat esetleges módositások következnek. Jóváhagyás után tervdokumentáció készitése, illetve ennek alapján a kivitelezés megkezdése.
A számitóközpontok védelmével kapcsolatos egyik legkülönlegesebb feladat a belépés-ellenőrzés megoldása. A témakör zárásaként ezt a különösen fontos területet érinteném, ill. az általunk megismert lehetőségeket ismertetném.

Ahhoz, hogy a belépés-ellenőrzés jelenlegi lehetőségeit áttekinthessük, egy rövid, nagyon durva történelmi áttekintést kell tennünk. Általában milyen lehetőségek vannak illetéktelen személy belépésének ellenőrzésére?

Belépés-ellenőrzés kulccsal.
A legelterjedtebben és évszázadok óta alkalmazott belépés-

ellenőrzés a mechanikus zár kulccsal. Ez a zárási mód, amely manapság csaknem tökéletes megoldást nyujt, mégsem tud bizonyos biztonsági követelményeket kielégiteni. Pl.:

- a zárás elfelejtése
- a kulcs elvesztése
- hiányzó rugalmasság a zárási terv kialakitásánál, amely személyi kulcsok esetében a belépési zónák behatárolására vonatkozna
- nincs lehetőség időbeli belépés korlátozásra és a be- és kilépések jegyzőkönyvezésére

Belépés-ellenőrzés személyek által.

Ez a megoldás is szigoru korlátokba ütközik, mindenek előtt ha egyidejüleg nagymennyiségü belépési módot és sok embert kell ellenőrizni.

Egy időszakosan gyakorolt ellenőrzést - pl. munkakezdéskor és végzéskor - nem lehet valóságos belépés-ellenőrzésnek nevezni.

Ehhez csatlakozik még, hogy az ember hosszabb idejü ellenőrzési feladat végzése alkalmával bizonyos elfáradási hatások lépnek fel, melyek a megfelelő negativ következményeket is magukkal hozzák.

Egy 24 órás, személyekkel megoldott ellenőrzés jelentős költséggel valósitható meg.

Belépés-ellenőrzés elektronikus ellenőrző rendszerrel.

Az elektronikus rendszerek ezen a területen is a legmodernebb, legegyszerübb, legbiztonságosabb és legésszerübb lehetőségét adják a belépés-ellenőrzés megvalósitására.

Egy ilyen rendszer a következő feladatokat tudja elvállalni:

- Az objektumon belüli személyforgalmat helyiségek szerint és idő szerint 24 órában szabályozza.
- A vezetők és a biztonsági személyzet mentesithető a belépés-ellenőrzés alól.
- A dolgozók számára a munkát megkönnyiti.
- Véd a lehetséges kockázat ellen.

Egy elektronikus belépés-ellenőrző rendszerrel szemben támasztott legfontosabb követelmények:

- az alkalmazó számára könnyü kezelési lehetőség,
- müködési és üzembiztonság,
- nagyon jó alkalmazkodás az objektum sajátosságaihoz,
- gazdaságosság.

A fenti rövid felsorolás szerinti értékelés messzemenően az elektronikus rendszerek előnyeit sejteti. Mégis mielőtt az elektronikus rendszer sajátosságaiba és lehetőségeibe mélyebben bele mennénk, hadd emlitsem meg a legősibb módszer legujabb eredményét is. A kulccsal való belépés-ellenőrzésnél emlitett hátrányok legnagyobbrészt a hagyományos zárakra és kulcsokra vonatkoznak. A zártechnika területén legujabb eredményként elért lehetőség a mágnesesen kódolt kulcsok és zárak előnyeiben testesül meg.
Hazai, jelentős importpótló eszközként kell megemliteni, az Elzett gyár legkorszerübb termékeként forgalomba került mágnesesen kódolt cilinderzár betéteket. Ezek a zárak jelentősen nagyobb biztonságot nyujtanak, a korábbiakkal összevetve. Miből származnak ezek az előnyök?

- a kulcs csak a gyár által sokszorositható, másolható,
- a kódolt információ nem olvasható ki,
- a fentiekből következően egy kulcs elvesztése már nem

jár akkora kockázattal, mint korábban,

- nincs kopó alkatrész, a mechanikus igénybevétellel összefüggésben, igy zárrendszereknél a korábbi stiftes rendszernél egy bizonyos idő után előállt un. összekopás itt teljesen kizárt,
- zárrendszerek kialakitása - az eddig legkorszerübbnek mondott Kaba-zárakhoz hasonlóan - egyszerüen megvalósitható,
- a hagyományos cilinder zárak helyébe minden átalakitás nélkül beszerelhető,
- a csapos rendszerü záraknál viszonylag egyszerü, de durva mechanikus behatással a hatástalanitás megoldható volt, ennél a zárnál ez is bonyolultabbá vált az erőszakos behatolást megkisérlő számára.

Természetesen továbbra is megmaradnak azok a hátrányok, melyeka kulcs jellegéhez kötődnek: rugalmasság hiánya, időbeli korlátozás, ill. be- és kilépések jegyzőkönyvezésének lehetősége itt sem megoldott.

A zár olcsósága és a fent emlitett előnyökből következő magasabb biztonság feltétlen indokolttá teszi, hogy a szakemberek az alkalmazás lehetőségét minden egyes esetben végiggondolják.

Ezután a kitérő után térjünk vissza az elektronikus belépés-ellenőrző rendszer lehetőségeihez és megoldásaihoz. Az itt ismertetésre kerülő rendszer a Cerberus Sensor Check System. Ez az elektronikus belépés-ellenőrző rendszer jelentős "láthatatlan" előnyökkel rendelkezik. A Cerberus Sensor Check System alapjában különbözik a hagyományos rendszerektől abban, hogy nagy alkalmazási kényelmet és ma-

gas biztonságot nyujt.

Ez a rendszer érintés nélkül müködik.
Ez azt jelenti, hogy az igazolványt nem kell egy leolvasó készülékbe betolni, hanem a láthatatlan érzékelő, igazolvánnyal való megközelitése következtében az igazolványban kódolt információ érintés nélkül kerül kiértékelésre.

Előnyei:
- Nem szükséges a Sensor Check igazolványt a kézben tartani. Pl. a ruhára rögzithető a leolvasó érzékelő magasságával egymagasságban.
- Mindkét kéz szabadon maradhat, iratok, vagy adathordozók szállitása, ill. egyéb célból.
- Elegendő az érzékelő megközelitése és jogosultság esetén az ajtó reteszelése foldoldódik, a belépést lehetővé téve.
- Az érzékelő sérülése, ill. szabotázsa csekély lehetőségü.
- Az érzékelő láthatatlanul is szerelhető.
- Nincs nyilása, melyet valamilyen tárggyal el lehet tömni, vagy meg lehetne sérteni.
- Robosztus kivitelü, a környezeti behatások ellen - időjárás, nedvesség, por - erősen védett.

Ezek a paraméterek nagy müködési biztonságot és gazdaságosságot nyujtanak.

A Cerberus Sensor Check System durva felépitése:

Az igazolvány:
A bérletméretü igazolvány láthatatlan tárolt kódokat tartalmaz, melyek egy adott személyre vonatkozó belépési jogosultságot határozzák meg, egy, vagy több helyiségre, ill. idő-

szakra vonatkozóan. Az Amerikai Egyesült Államok Energiaügyi Minisztériumának vizsgálatai szerint ez a kártya nagyobb biztonsággal rendelkezik, mint a vele összehasonlitható rendszerek. A komplex kód számitógép vezérelt véletlen - algoritmus alapján kerül meghatározásra. A biztonság még tovább fokozható kombinációs kód segitségével, bármely kártyánál.

Elvesztés, vagy ellopás esetén egyes kártyákat, vagy egész igazolvány csoportokat a központról azonnal le lehet tiltani. Ezzel a megtaláló, vagy a tolvaj számára a kártya értéktelenné tehető.

Az egyes igazolványokat a feladatok és a felelősség hatásköre szerint egyénenként külön-külön lehet térben és időben érvényesiteni. A belépési jogosultság mértékét ezek alapján meghatározni. Az igazolványok tetszőlegesen feliratozhatók; cég neve, cime, dolgozó neve, fényképe stb. Biztonsági okokból általában a legcélszerübb az igazolványt üresen hagyni.

Érzékelő:

Az érzékelő egy négyszögletes müanyag lap, mozgó alkatrész nélkül. Látható és láthatatlan szerelése egyaránt megoldható pl. falboritás alá, vagy ajtóba szerelve. El lehet látni különböző fényjelzőkkel is a visszajelzés biztositása érdekében.

Ez az érzékelő mintegy 10 cm távolságban már leolvassa az igazolványban tárolt és kódolt információkat. Szabad térben való szerelése is megoldott minus 15C°-tól +50 C° hőmérsékletig, 100 % légnedvesség mellett.

A rendszer:

Az érzékelő az igazolványban tárolt információkat továbbitja a központhoz. A központ ellenőrzi a információt, a helyre és időre vonatkozó belépési jogosultság szerint és egyezés esetén vezérli a speciális ajtóellenőrző, ill. ajtóvezérlő modult, mely az ajtók minden tipusához - ajtószárnyak, forgóajtók, forgókeresztek és zsilipek - alkalmazhatók.
A rendszer moduláris felépitésü, igy az igényeknek megfelelően, ill. a beruházási lehetőségekből következően fokozatos kiépitést is lehetővé teszi. A legbonyolultabb kiépitéshez a rendszerben programozó készülék áll rendelkezésre, az egyes igazolványok érvényesitésére, ill. érvénytelenitésére: lehetőség van térben és időben való jogosultság megadására, ennek módositására, ill. törlésére. A rendszerhez szalagnyomtató csatlakoztatható, melyen a következő adatok nyomtathatók ki: dátum, idő, igazolványszám, belépés helye, belépési jogosultság.

Remélem, hogy ez a példaként kiragadott vagyonvédelmi lehetőség, mely olcsóbb és drágább kivitelben egyaránt megvalósitható, elegendő volt ahhoz, hogy a számitóközpontok speciális biztonságtechnikai kérdései iránt az érdeklődést felkeltsem. A GELKA vagyonvédelem minden érdeklődő számára kész a továbbiakban mélyebb, részletesebb felvilágositást és információt adni, a saját szakterületén aktuális vagyonvédelmi problémák megoldásához.

Horváth Pál:

ADATVÉDELEM A TÁVADATFELDOLGOZÁSBAN

Bevezetés

Érdekeiből kiindulva az ember óv, véd mindent, ami számára érték. Korunk rohamosan növekvő értéke az információ. Védelme - különösen a vizsgálatunk tárgyát képező szállitás, az adatátviteli, terén - feladatot jelent az információs rendszerek tervezői, készitői, üzemeltetői és használói számára egyaránt.

Az információ védelme egyáltalán nem napjaink uj szükséglete. A ma ismert legkorábbi titkositási eljárásokat az egyiptomi uralkodók használták 4000 évvel ezelőtt. Jellemző a probléma fontosságára, hogy alig öt évvel a telefon szabadalmaztatása után, 1881-ben már kidolgozták a beszédscramblert, ami érthetetlenné téve a beszédet, megvédte azt a lehallgatástól. A mind ujabb megoldások kidolgozása napjainkban is folytatódik. Közülük egy nagyon szellemes megoldás a nyilt kulcsu rejtjelezési rendszer.

Az idők során módosult a titkositott információ jellege is: régen elsősorban a katonai és diplomáciai téren alkalmazták, ma pedig széleskörü alkalmazásra talál az ipar, kereskedelem, pénzügyi élet, államigazgatás stb. területén is. Mivel mindezek a szférák intenziv távközlési, és ezen belül adatátviteli felhasználók is, az adatvédelem a távadatfeldolgozás lényeges részévé vált.

Távadatfeldolgozás és adatvédelem

Az adatok távközlési hálózatra való kijuttatása megkönnyiti a jogosulatlan hozzáférést. Ennek következménye lehet a személyiséghez füződő jogok sérelme, anyagi kár, a nemzetbiz-

tonság kára, stb. Sok országban ezért adatvédelmi törvényeket hoztak, melyek célja alapvetően a személyiséghez füződő jogok védelme. Mivel az országok nem egységesen szabályozzák az adatvédelem kérdéseit, az eltérések bizonyára hatással lesznek a nemzeti adatfeldolgozó iparok külföldiek részéről történő felhasználása terén. Megvan az esélye annak, hogy az un. adóparadicsomokhoz hasonlóan az eltérő szabályozásból fakadóan adatparadicsomok is létrejönnek. Ennek előjelei és előfeltételei már megvannak, hiszen hatalmas adattömegek mozognak máris az országhatárokon át, nem kis fejfájást okozva egyes országok kormányainak. Nyilvánvaló ugyanis, hogy amennyiben egy ország adatait jelentős mértékben külföldön dolgozzák fel, ott tárolják, vagy, ha valamely ország tulzottan a külföldi adatbázisok használatára alapozza kutatásait és fejlesztéseit, akkor függő helyzetbe kerül a szolgáltatást nyujtó országtól. Az adatvédelmi törvények ezért szabályozni igyekeznek a nemzetközi adatforgalmat. Személyi adatok kivitelét például akkor engedik meg, ha a célországban is hasonló elvü adatvédelmi törvény van érvényben. Külön gondot jelent, hogy mig minden ország rendelkezik vámelőirásokkal a valamilyen hordozóra rögzitett információ /könyv, magazin, ujság, film, hang- vagy videokazetta, stb./ forgalmazása, addig az értékkel ugyancsak rendelkező, de adatátviteli uton a határt átlépő információ "vámolására" nincsenek kidolgozva a szabályok és módszerek.

Az adatvédelem szempontjából a távadatfeldolgozó rendszerek három alapvető elemét különböztetjük meg:

- számitógép

  biztositható a számitógép védett elhelyezése, az objektumon belül az adatok a teljes számitástechnikai rendszer védettségétől függően - akár

nyilt formában is - tárolhatók, szabályozandó az adattárolók használatának módja és meg kell oldani a felhasználók azonositását,

- adatátviteli vonal /hálózat/

kiterjedése és megvalósitási módja miatt fizikailag nem védhető megfelelő mértékben, ha az átviteli ut nem védhető, akkor a rajta átvitt információt kell védeni, az információvédelem módja: az információt érthetetlenné tenni a nemkivánatos felhasználók számára,

- terminál

a fizikai védelem a terminálok száma és elhelyezése miatt gyakran nehezen megoldható, de esetenként elkerülhetetlen feladat; általában szükséges a felhasználók azonosithatatlanságának a biztositása a behatolók /pl. vonalat lehallgatók/ számára.

Az átviteli utra kijuttatott információ érthetetlenné tételénél alapelv, hogy az információt védelmi céllal olyan mértékben torzitsuk el, hogy a megfejtéséhez szükséges idő- és pénzráforditás aránytalanul magas legyen az információ elavulási idejéhez és értékéhez képest. A nemkivánatos beavatkozás azonban nemcsak a védett információ megszerzésével és megfejtésével, hanem információnak a rendszerből való kivonásával /a rendeltetési helyre való eljutás megakadályozásával/, korábbi adatoknak a rendszerbe történő visszajuttatásával, vagy a kommunikáló partnerek valamelyike szerepének a szimulálásával is képes zavart okozni. A legveszélyesebb - de legnehezebben megvalósitható is - a legutóbbi, mert egyaránt módot ad információszerzésre és félrevezetésre.

A vonali adatvédelem a rejtjelezés utján történik. A rejtjelezés egy E /elrejtés/, D /megfejtés/ transzformációpár alkalmazását jelenti. A hatékony, nehezen megfejthető transzformáció bonyolult berendezést igényel. Ez károsan befolyásolja a berendezés árát, méreteit, használhatóságát. A rejtjelező rendszerekben ezért a transzformációk jelentős része nyilt és rögzitett, az eszköz felépitése tehát a védettséget kevéssé érinti. A transzformáció titkosan kezelt, kisebb, változó komponense csak a rejtjelezés időtartamára kapcsolódik a nyilt részhez. Ez a komponens a kulcs, mely elég nagy értéktartományból kell, hogy választható legyen annak érdekében, hogy a halmaz elemeinek kimeritéses sorravételével történő megfejtési kisérlet ne legyen célravezető. A kulcsválasztás nagy értéktartománya szükséges ahhoz is, hogy védett rendszereken belül a nagyszámu kapcsolat egymástól is védett legyen. Szükséges, hogy a rejtjelezés megfejtésére egyedül a kimeritéses sorravételezés legyen a célravezető stratégia.

A fentiek miatt a kulcs szerepe kiemelkedően nagy, és a teljes rendszer védettségét a kulcs védettsége határozza meg. A kulcs a használat több fázisában van kitéve az eltulajdonitás veszélyének:

- előállitás,
- tárolás,
- továbbitás.

A továbbitás, az un. kulcs kiosztás fázisa legsérülékenyebb. A kulcskiosztásra ugyanaz a közeg áll rendelkezésre, amelyen a védett adatforgalom is folyik. A kulcsokat ezért valamely kulcsvédelmi kulcsrendszerrel kell óvni. Mivel ez a fázis a bonyolultság magasabb szintjén is a rendszer müködésének kritikus része marad, a vázolt problémák kiküszöbölésére irányuló kutatások elvezettek az emlitett nyilt kulcsu rendszerekhez. Ezen rendszerek esetében maga a kulcs ismert, de

az E transzformáció ismeretében a D gyakorlatilag megállapithatatlan.

A rejtjelező eljárások nemcsak az információ eltulajdonitása, hanem megváltoztatása, visszajuttatása, eltéritése ellen is védelmet biztositanak, és az információ hitelesitésére is használhatók.

A rejtjelezés nagyon kétélü fegyver. Veszéllyel jár valamely kereskedelmi forgalomban lévő /pl. nyugatról importált/ rejtjelező készülék használata is, mivel ez a rejtjelező kiszolgáltatottságát jelenti a gyártónak vagy forgalmazónak és esetleges megbizóinak. Ezen veszélyeket figyelembe véve a kérdést hazánkban szabályozó 1/1981. BM. számu rendelet csak a Belügyminisztérium illetékes szerveinek engedélyével, az általa meghatározott módon teszi lehetővé rejtjelezés alkalmazását.

Az adatbiztonság megsérülésének müszaki feltételei a távközlési rendszeren belül

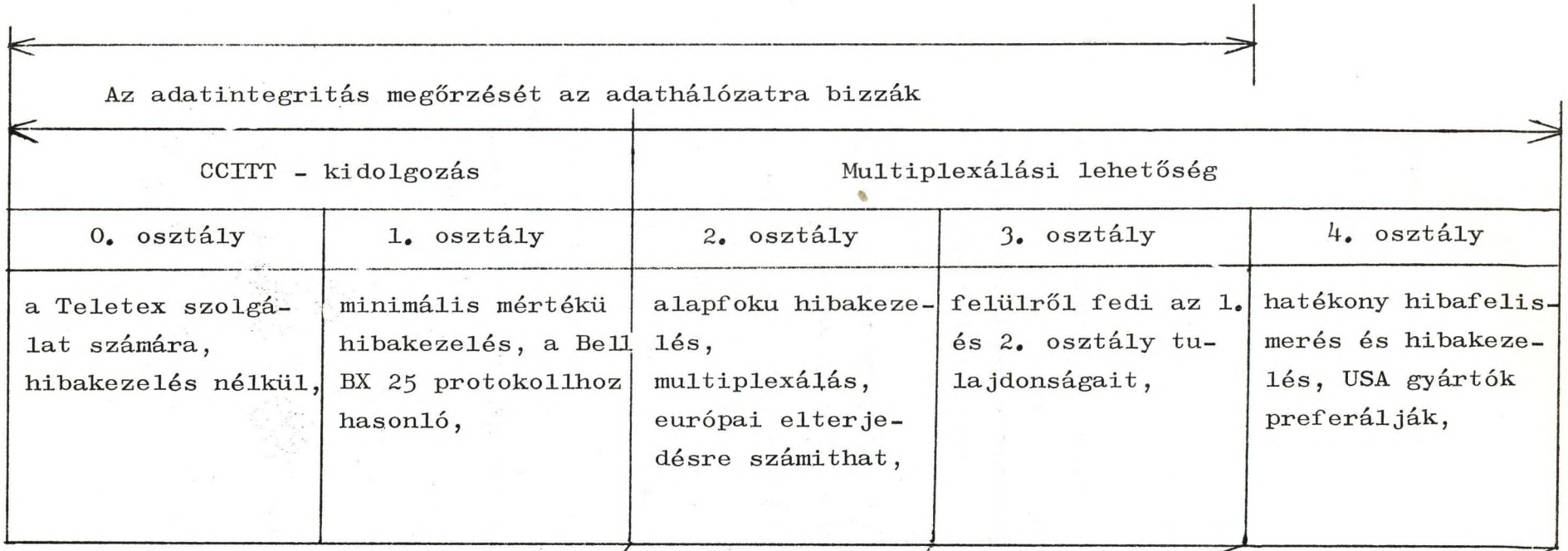
A távközlési rendszerek átviteli utakból /szimmetrikus érpár, légvezeték, koaxiális kábel, fényvezető éter stb./, átviteltechnikai berendezésekből és /kapcsolt hálózat esetén/ kapcsoló berendezésekből állnak. Mindezen komponensek helytelen müködése, vagy az ezekbe való illetéktelen beavatkozás oka lehet az adatbiztonság megsérülésének. Vegyük sorra először a távközlési rendszer tulajdonságaiból fakadó, az adatbiztonságot veszélyeztető jelenségeket.

A távközlési rendszerek mindhárom komponensében keletkezhet áthallás a rendszeren belül üzemelő érpárokra, csatornákra, összeköttetésekre. Távbeszélő központokban, helyi kábelekben a parazita csatolások, frekvenciamultiplex átviteltechnikai rendszerekben a nemlinearitások lehetnek áthallás okozói.

A lehallgatásra módot ad a kábelek nagy kiterjedéséből fakadó védetlensége, a mikrohullámu összeköttetéseken a nyaláb szóródása, esetleg maguknak a távközlési eszközöknek vagy az adatvégberendezéseknek a nemkivánatos elektromágneses sugárzása.

A kapcsolódó központok a hivások valamely igen kis részét tévesen kezelik. A helytelen müködés eredménye lehet téves kapcsolás, hivás-összeakadás /kettőnél több partner nemkivánatos felkapcsolódása egyetlen összeköttetésre/, üzenetek vagy adatcsomagok téves cimre irányitása stb. Jogosan merül fel a kérdés, hogy mennyire szabad bizni az igénybevett távközlési szolgáltatás megbizhatóságában. Alapelvként jobb, ha ugy tekintjük, hogy semennyire. Pontosabb megfogalmazást keresve állithatjuk, hogy az átvitt információ értékének, fontosságának vagy titkosságának mértékével forditot arányban. Ebben a kérdésben ellentétes véleményen vannak az ISO /alapvetően európai/ és az USA NBS /National Bureau of Standards/ transport /szállitási/ protokoll szabványositói. Az ISO kétszintü nyilt hálózati architekturájában a szállitási szint feladata az adathálózatot jelentő alsó három szint jellemzőinek elfedése a magasabb szintek számára. A szállitási protokoll a legalacsonyabb szintü end-to-end protokoll. Az európai nézet szerint az adathálózatok megbizhatóak és a legtöbb információfajta átvitele nem igényli a hálózati zavarok transzport szinten megvalósitott lekezelését. Ezzel szemben az amerikai nézet a maximálisan bizalmatlanságból indul ki, elvégzi a csomagok sorrendezését /amit az alatta levő hálózati szint is elvégez/ és az elbontott adathálózati összeköttetést felépiti anélkül, hogy azt a felsőbb szintek észrevennék. A különböző szállitási osztályok funkcióit a következő ábra szemlélteti.

Az ISO szállitási protokoll osztályai



Az NBS szállitási protokoll osztályai

Alapfoku	Bővitett
megbizható hálózatot feltételez, ISO komatibilis, a bővitett osztály valódi alosztálya	hibafelismerés/-elhárítás, ismételt, elveszett, sorrendhibás, hibás csomagok felismerése, véletlenül elbomlott kapcsolat felépitése, az ISO 4. osztályánál több funkcióval rendelkezik,

1. ábra. Az ISO és az NBS szállitási protokoll osztályai /Edvin E. Meier cikke nyomán, Data Communications 1982. julius/

Az adatátvitel biztonságának biztositása

Az adatátviteli rendszerbe való behatolás tárgya lehet vagy valamely távközlési rendeltetésü eszköz /hardware vagy software/, vagy maga az átvitt információ.
A távközlési rendszerbe való behatolás célja lehet
- a müködés zavarása, pl. elektromágneses zavarás révén,
- a müködés megakadályozása, pl. a tápellátás megszüntetése, kábel elvágása stb.,
- lényeges rendszerelemek megsemmisitése,
- a rendszer müködési módjának módositása, pl. tárolt program vezérlésü rendszer átprogramozása.

A posták többszörösen biztositott tápellátással, objektumaik védelmével, gyors kerülőutképzéssel és a software módositás jogosultsághoz kötésével védekeznek a behatolás ellen. Az információ megtámadásának módjai:

- nem kivánatos passziv részvétel az információ forgalomban /lehallgatás, forgalmi jellemzők elemzése, rejtjelezés megfejtése/,

- nem kivánatos aktiv részvétel az információ forgalomban /információ kivonása a közegből, az információ késleltetett és/vagy torzitott bevitele /visszavitele/ a rendszerbe, a kommunikáló partnerek valamelyike szerepének az átvétele/.

Az ilyen és ehhez hasonló zavartatások kiküszöbölését célzó távközlési biztonsági módszerek feladatai:

a. az üzenettartalom nyilvánosságra kerülésének megakadályozása,

b. a forgalomelemzés lehetetlenné tétele,

c. az üzenetfolyam módositásának felfedezése,

d. hamis üzenetnyelők /információ kivonása a rendszerből hamis pozitiv válaszok visszaküldése révén/ felfedése,

e. hamis kapcsolatfelépitès kimutatása.

A lehetséges védekezési módok:

a. rejtjelezés;

b. folyamatos, rejtjelezett üzenetek hiján attól megkülönböztethetetlen kitöltő bitfolyam átvitele; nyilvános kapcsolt hálózatokon ez a megoldás nem alkalmazható, ott inkább a forgalomelemzés eredményeit meghamisitó ál-forgalom generálása lehet megoldás;

c. szükséges az üzenetforrás azonositása, az üzenet integritásának ellenőrzése, a blokkok sorrendezésének és küldési idejének az ellenőrizhetősége;

d. titkositott párbeszédes protokoll alkalmazandó;

e. megbizható partner azonositás szükséges.

A rejtjelezés valamennyi módszernek lényeges eleme.

Az uj távközlési szolgálatok és müszaki megoldások által felvetett adatvédelmi problémák

A telex szolgálat esetében az információátvitel a TTX terminálok memóriái között megy végbe. Kikapcsolódik tehát a szövegkommunikációból minden, a telex esetében az ember legalább egyik oldalon történő jelenlétéből fakadó kontroll lehetősége. Ennek pótlására a TTX szolgálatban a következő biztonsági megoldások bevezetésével foglalkozik a CCITT:

- elektronikus aláirás: egy üzenet mező, amely azonositja a küldőt, és felderithetővé teszi a hálózatban történt üzenetmódositást;

- a rejtjelkulcsok automatikus kezelése;
- zárt előfizetői csoport képzése a viszony /session/ szinten, ilyen szolgáltatást a nyilvános adathálózatok is nyujtanak a hálózati szinten, azonban a korábbiak értelmében egyes hálózati funkciók a bizalmatlanság jegyében a magasabb szinteken megismétlődhetnek;
- kulcsszó /password/ alkalmazása viszony szinten.

Az adatbankok használói ki vannak téve annak a veszélynek, hogy adatforgalmuk megfigyelésével meghatározzák az információs profiljukat. Egy kutatóintézet esetében ugyanis a folyó kutatások irányára és előrehaladottságára jól lehet következtetni a használt adatbankokból és a lekért információból. Szükséges tehát a tényleges célok elfedését célzó, a forgalomelemzőket félrevezető lekérdezési taktika.
Az adatfolyamok ellenőrzését nehezíti meg a csomagkapcsolt adathálózatok adaptiv irányitási rendszere. További problémát jelent ezen a téren, hogy a digitális beszéd bitfolyama és a titkositott adatfolyam csak igen nehezen különböztethető meg egymástól.
Ugyancsak az adatfolyamok ellenőrzését akadályozza a közvetlen müholdas adatátvitel elterjedése. Realitássá vált a kapcsoló központok világürbe telepitése /"switchboard in the sky"/, sőt, maguk az adatfeldolgozó, vagy adatbank-szolgáltatást nyujtó számitógépek is elhelyezkedhetnek ürállomásokon. Az emlitett müholdas megoldások különösen az országhatárokat átlépő bitfolyamok esetében jelentenek egyelőre alig belátható müszaki és jogi problémákat.

Az adatvédelem helye a nyilt hálózati architekturában

A korábbiak szerint adatvédelmi funkciók a nyilt hálózati architektura több szintjén is megvalósulnak.

A hálózati szint zárt előfizetői csoport képzését, valamint a hivó és a hivott vonal azonositását biztositja. A szállitási szint - ha igény van rá - csomagsorrendezést végez. A viszony szinten zárt előfizetői csoport képezhető, kulcsszó használata is előirható.
A rejtjelezés nyilt hálózati architekturában való elhelyezése nem eldöntött kérdés. Valószinüleg a viszony vagy a megjelenitési réteg feladatává fog válni a rejtjelezés. Javaslat van az adatkapcsolati szintü megvalósitásra is, ez azonban tul sok hátránnyal jár: a távközlési szolgáltató is be lenne avatva a titkositásba, a szállitási szintnek tudnia kellene a védett adatkapcsolatokat kiválasztania, módositani kellene a már kialakult hálózati és szállitási protokollokat. Jelenleg, a nem nyilt hálózati alkalmazásokban a kereskedelemben forgalmazott eszközökkel a fizikai szinten történik a titkositás. Ez magyarázza az eszközök jellemzői között általában felsorolt "protokoll átlátszó" jelzőt.

Réh János:

FIZIKAI BIZTONSÁGOT SZOLGÁLÓ INTÉZKEDÉSEK A SZÁMITÓKÖZPONTOK TERVEZÉSÉNÉL, TELEPITÉSÉNÉL ÉS ÜZEMELTETÉSÉNÉL

Az elmult 8-10 évben az SZKFP keretén belül több mint 15 milliárd forintot forditottunk számitógépparkunk fejlesztésére.
A telepitett rendszerek sajátossága, hogy igen kis területen 50-150 m²-en igen nagy érték koncentrálódik.

Ha a közép-nagykategóriáju gépeket vizsgáljuk, megállapitható, hogy 350-550.000,- Ft/m² értékkoncentrációt kell figyelembevennünk.
A számitógépes szakma fejlődésének olyan szakaszába jutottunk, ahol már a biztonságot nem szabad elhanyagolnunk, létrehozott értékeinket védeni szükséges.

A közelmultban megjelent 1/1981. BM rendelet megfelelően szabályozza a számitástechnikai rendszerek titok-, vagyon- és tüzvédelmét. A rendelet végrehajtása érdekében igen sokat lehet és kell tennünk.

A számitástechnikai rendszerek értéke magábafoglalja a gép + környezet + adathordozók + felhasználói módszerek és a fejlesztés költségeit is.

A fizikai védelem igen jelentős szerepet játszik, az adminisztrativ kontroll, az adatfeldolgozás biztonsági rendszere, és a jogi szabályozás összefüggő ellenőrzési rendszerében.

A korábban emlitett rendelet végrehajtása során a fizikai biztonságot célszerüen szolgáló intézkedések sorozatát kell foganatositanunk a tüzvédelem, vagyonvédelem, klimatizálás,

energiaellátás, belépésellenőrzés, mágnesszalag és lemezkezelés területén.

A számitóközpont szémára a fizikai biztonság zárt ellenőrzött biztonságos környezetet jelent, melynek megteremtése komplex tevékenység, amely a kockázatelemzésen elapul, magába foglalja a különböző lehetséges veszélyek valószinü gyakoriságát és következményeit a lehetséges veszteségek költségeit.

A fizika biztonság megteremtése számos költséges intézkedést és megfelelő berendezések alkalmazását teszi szükségessé.

Igen fontos, hogy a kockázati faktorok és az alkalmazásra kerülő technikai értéke arányban álljon.

A következőkben a teljességre való törekvés igénye nélkül szeretném összefoglalóan ismertetni mind a passziv, mind az aktiv intézkedések sorát, amelyet a számitóközpontokat üzemeltetők figyelmébe ajánlok.

Tüzvédelmi feladatok számitóközpontok létesitésének előkészitésénél

A BM rendeletnek és KSH elnöki irányelveknek megfelelően alapbiztonsági és fokozott biztonsági kategóriákban differendiáltan kell eljárni.

Kiegészitő biztonsági intézkedéseket kötelezően csak a titkot képező adatokkal folyamatosan,illetve előreláthatóan ismétlődő rendszerességgel munkát végző szerveknél kell foganatositani.

Ilyen esetekben már a számitóközpont telepitésének előkészitési /tervezési/ szakaszában intézkedni kell a különleges tüz és vagyonvédelem, biztonsági, jelző és riasztó berendezések alkalmazására.

Intézkedni kell továbbá a kivitelezés módját és minőségét meghatározó általános érvényü előirások figyelembevételére, amelyek a szakhatósági jóváhagyásokat lehetővé teszik.

A feladatok ellátásához egyrészt passziv, másrészt aktiv intézkedéseket kell tennünk.

Passziv tüzvédelmi intézkedések
/a BM MI-02 102-79. müszaki irányelvek alapján/

Épitészeti kialakitás - elhelyezés

- Legkedvezőbb a földszinti vagy I. emeleti számitógépterem elhelyezés.
- A számitógéptermet magában foglaló tüzszakaszon belüli térelválasztó megengedett /fém-üveg kombinációs térelemekkel/
- A számitóközpont "D" tüzveszélyességi osztályba tartozó létesitmény.

Számitógépkörnyezet belső kialakitása

- Számitógépterem hő- és hangszigetelésére csak nem éghető anyag használható.
- Álpadló, álmennyezet tartószerkezete nem éghető, burkolata pedig nehezen éghető lehet.
- Adathordozók tárolására szolgáló helyiséget célszerü önálló tüzszakaszként kialakitani.

- Az álmennyezetben és az álpadlóban, ahol villamos vezeték huzódik, tüzoltás céljából jelzett mezők kialakitása indokolt, oly módon, hogy azok könnyen megbonthatók legyenek.

Épületgépészet

- Gáz, gőz és vizszállitó vezetékeket nem szabad a gépterem átvezetni.
- A tüzgátló szerkezeteken átvezető légtechnikai vezeték nem éghető anyagból készüljön, tüzszakaszhatárnál önmüködő elzáró berendezéssel legyen ellátva, melyet a tüzjelző berendezés vezérel.
- Klimaberendezést számitógépteremben és számitógéptermen kivül is el lehet helyezni.

Villamosság

- Számitógépterem és klimagépház áramellátása legalább két helyről legyen megszakitható, egyik megszakitási lehetőség a számitógépterem bejárata közelében legyen.
- Fénycsővilágitás esetén csak olajszigetelés nélküli kondenzátor kerüljön alkalmazásra.
- Az üzemi világitáson kivül vészvilágitás és irányfény alkalmazása indokolt.

Aktiv tüzvédelmi intézkedések

- A számitóközpontban indokolt esetben, továbbá, ha a tüzvédelmi hatóság előirja, tüzvédelmi automatika, önmüködő tüzjelző és vezérlő, illetve oltó berendezés létesitendő.
- A keletkező tüz oltására halonnal vagy CO_2-vel oltó kézi tüzoltó berendezéseket kell elhelyezni, a gépterem bejá-

ratánál, a géptermen belül, a nagyobb tüzkockázatu gépegységek közelében.

A következőkben a fizikai biztonság gyakorlati megvalósitásáról szeretnék szólni.

Gyakorlati intézkedések a fizikai biztonság megvalósitására

Az esetleges veszélyek időbeni felismerésére tüz-, füst, hőmérséklet és páratartalom érzékelő, továbbá behatolás és betörésjelző készülékeket szükséges alkalmazni.
A behatolásjelző készülékek riasztórendszer-beállitását a területileg illetékes rendőri szervekkel előzetesen egyeztetni kell.

Tüz megelőzése

Az előzőekben vázolt passziv és aktiv tüzvédelmi intézkedéseken tulmenően szükséges további intézkedéseket foganatositani a tüz megelőzésére.

A berendezések, az álpadló alatti terek tisztántartása és programszerü ellenőrzése, a személyzet tüzvédelmi oktatása, fontos feladat.
A gépteremben nem szabad nagyobb mennyiségü papiralapu adathordozót tárolni /csak napi feldolgozáshoz szükségest/.

Vizkár megelőzése

A klimaberendezések üzeméhez használt vizmennyiség vezetésére gondot kell forditanunk. Az esetlegesen a számitógéptermen áthaladó vizvezetékeket ki kell váltani.

Külső vizbetörések /árviz/ elleni védekezés szempontjait figyelembe kell venni.

Belépés-ellenőrzés

Az a felismerés, hogy egy számitóközpontot a külvilágtól nem lehet hermetikusan elzárni, szükségessé teszi az illetéktelen belépés elleni biztonsági intézkedések megtételét. A gyakorlatban célszerü hardware, software és adatkezelési zónákat kialakitani, mely zónákba csak az ott dolgozók belépését engedélyezzük.

A belépés-ellenőrző rendszerek közül legjobban a mágneskártyás, illetve számjelkódos berendezések terjedtek el.

A belépés-ellenőrzés vonatkozásában nem az a döntő, hogy milyen sok pénzt költöttünk bonyolult biztonsági berendezésre, hanem az a fontos, hogy ne hagyjunk figyelmen kivül olyan egyszerü folyamatokat, amelyek hatástalanithatják a belépés-ellenőrzési rendszert.

Biztonságos energiaellátás

A folyamatos számitógépüzem realizálása igen nagymértékben függ a zavarmentes energiaellátástól.

Amennyiben a számitógépet ellátó hálózaton különböző zavarok mutatkoznak /hálózat-kimaradás, impulzuszavar, frekvenciacsökkenés/, abban az esetben müszeres méréssel meggyőződhetünk a zavar okairól és intézkedéseket tehetünk a jelenség kiküszöbölésére.
Müszaki-gazdasági megfontolások alapján dönthetünk energiaellátó berendezések alkalmazásáról, pl. külön transzformátor, motorgenerátor, vagy szünetmentes áramforrás.

Az adathordozók tárolása

Mágneslemezen, szalagon, mikrofilmen és a papiralapu adathordozókon tárolt információk értéke felbecsülhetetlen.

Ezért az adathordozók biztonságos tárolására igen nagy gondot kell forditanunk. Hazai viszonylatban problémát okoz, hogy az adathordozók védelmét szolgáló tüzbiztos tárolószekrények nem állnak rendelkezésre.
A papiralapu adathordozók védelmét olyan tárolószekrényekkel tudjuk megoldani, amelyek a belső hőmérsékletet olyan szinten tartják, amelynél az adathordozók még nem kezdenek barnulni, ill. pörkölődni. Mágneses adathordozók esetén a hőfokot a szalag károsodási hőmérséklete alatt kell tartani. Ugyancsak fontos, hogy a mikrofilmek tárolására szolgáló szekrények is megfelelően védjék az adathordozót a károsodástól.

Mivel az adathordozók védelme fontos láncszem a fizikai biztonság létrehozásában, sulyt kell fektetni a megfelelő védelemre.

AZ ADATVÉDELEM PROGRAMOZÁS- ÉS ÜZEMELTETÉSTECHNOLÓGIAI KÉRDÉSEI

István Lajos:

ÜZEMELTETÉS- ÉS PROGRAMOZÁS-TECHNIKAI ELJÁRÁSOK, ESZKÖZÖK AZ ADATVÉDELEM TERÜLETÉN

A számitógépes feldolgozásokkal kapcsolatos visszaélésekről, főleg angol és német nyelvü szakirodalomban elgondolkoztató statisztikát és előrejelzéseket olvashatunk, egyben tanulhatunk is belőlük.
Dr. Borda József a "Számitógépes rendszerek ellenőrzése és biztonsága" c. könyvében ezek egy részét csokorba foglalja. E felsorolás szinte kivétel nélkül valamelyik kapitalista országot érinti, de a mi társadalmi viszonyaink között is előfordulhat a számitógéppel kezelt adatok megsemmisülése és ezzel adott esetben felbecsülhetetlen kár keletkezhet.

Hazánkban a különböző intézményeknek és az állampolgároknak egyaránt törvényes joga és érdeke füződik a biztonságos, a szocialista jogi és erkölcsi normákat messzemenően figyelembe vevő gyakorlat kialakitásához. E gyakorlat megalapozását szolgálja a belügyminiszter 1/1981. /I.27./ számu rendelete, amelynek hatása kiterjed a számitástechnika-alkalmazás teljes folyamatára /üzemeltetés, programozás, adathordozók tárolása stb./, átfogja teljes technológiai láncát.
Az érvényben lévő vagyon- és tüzvédelmi szabályzatok mellett a rendelet fokozottabb védelmi követelményeket támaszt a nagyértékü számitóközpontok irányába.

Az előadás keretében nem vizsgáljuk a teljes technológiai láncot, csupán - időszabta korlátok miatt a teljesség mellőzésével - azok a programozás-technikai és üzemeltetési eljárások és ehhez kapcsolódóan azok a törekvések kerülnek bemutatásra, amelyeket az épitőipar, ezen belül elsősorban az Épitésgazdasági és Szervezési Intézet területén a rendelet megjelenése óta folyamatosan igyekszünk megvalósitani.

A védelem szervezésének helyi sajátosságai

Az adatvédelemmel kapcsolatos irodalom több olyan fogalmat használ, amely megfogalmazásában eltérő, de lényegét tekintve nem. Leggyakrabban az adatvédelem /privacy/ és adatbiztosítás /security/ kifejezésekkel találkozhatunk, ahol az előbbi arra ad választ, hogy "mit" kell megvédeni, mig az utóbbi azt mondja meg, "hogyan" kell megvédeni azokat. A rendelet megjelenése óta eltelt időszak tapasztalatai alapján állithatjuk, hogy egy rendszer adatvédelmének szervezése folyamatos és annak kiépitésével párhuzamosan folytatott rendszeres megelőző tevékenység. A védelem szervezésének kezdetén az Intézet sajátosságaiból indultunk ki.

Az ÉGSZI az Épitésügyi és Városfejlesztési Minisztérium bázisintézete. Tevékenységi köre társadalmi, közgazdasági, müszaki-gazdasági, valamint munka-, üzem-, vállalatszervezési kutatásokból, szervezésekből és az ezekhez kapcsolódó számitástechnikai szolgáltatásokból áll. Budapesten és öt vidéki városban összesen többszáz millió forint értékü számitástechnikai eszközállományunk van.

Jelenleg a következő számitógép tipusokat üzemeltetjük számitógép hálózatunkban: ESZ 1022, ESZ 1035, ESZ 1040, IBM 370, Siemens 4004, RC 3600, továbbá az MSZR kategóriából SZM-4, A 6401, VT 20 rendszerek.

Az intézeti programvagyon mintegy 200 mFt.

Számitástechnikai Védelmi Szabályzat /SZVSZ/

Az Intézet vezetője a rendelet megjelenése után Igazgatói Utasitással léptette életbe az intézeti SZVSZ-t.
A szabályzat fő fejezetként foglalkozik a számitástechnikai berendezések védelmével.

Ezek közül megemlitünk néhányat:

- meghatározza a számitóközpontok tervezésének, telepitésének szempontjait,
- irányt mutat a rendészeti vonatkozásu feladatokhoz, ezen belül kiemelten foglalkozik a számitógépüzem helyiségeibe történő be- és kilépés kérdéseivel és az illetéktelen behatolás elleni védelem tennivalóival,
- rendelkezik a tüzvédelem helyi sajátos feladatairól,
- előirja a müszaki ellátással szemben támasztott követelményeket,
- elrendeli az adathordozók beszerzésével, nyilvántartásával, tárolásával, szállitásával kapcsolatos teendőket,
- rendelkezik az adatvédelmi felelős jogállásáról,
- meghatározza a rendkivüli események bekövetkezése esetén foganatositandó intézkedéseket /katasztrófa-terv/.

A felsorolás nem teljes, hiszen nem célunk, hogy a megfelelő titkossági fokozattal ellátott intézeti SZVSZ-t részleteiben bemutassuk, ennek keretében csupán néhány gondolatot emelünk ki a védelmi rend szervezéséhez kapcsolódóan.

A fizikai védelem néhány kérdése

A számitástechnikai rendszerek védelmének fontos része a tüz- és vagyonvédelem.

A 4/1980. /XI.25./ BM számu rendelet, illetve a BM-TOP irányelvei alapján a számitógéptermek és közvetlen kiszolgáló egységeinek helyiségei "D" tüzveszélyességi osztályba tartoznak.

A tüzvédelem helyi feladatairól nálunk egy korábban kiadott Igazgatói Utasitás rendelkezik, amelynek kiegészitéseként a

számitógépüzemekre külön meghatározott sajátos előirások az SZVSZ egyik mellékletét képezik.

Dr. Matók György irja az "A számitógépes információs rendszerek ellenőrzése, biztonsága, gazdaságossága" cimü, még 1975-ben megjelent munkájában: "A számitógépek géptermére jellemző, hogy egy négyzetméternyi területére sok százezer forintnyi beruházott érték jut. Ennek tudatában kell megszervezni a biztonságot."

Véleményünk szerint is a védelem szervezésénél ez helyes szemlélet.

Az ÉGSZI-ben a többszáz milliós intézeti vagyon megóvása a kisebb és nagyobb károktól, a tüzvédelmi követelmények betartása, megvalósitása nem olcsó, de az ilyen koncentrált értékek védelme fokozott biztonságot követel. Az emlitett értékek megóvása egyben szakembereink átfogó és hosszabb távra szóló intézkedéseit igényli, amely magába foglalja a vagyon- és tüzvédelem teljeskörü megszervezését, a megfelelő, a feladatok ellátását megoldó technikai berendezések üzembeállitását.

Az utóbbi 1,5-2 éves időszak alatt főleg R-22-es rendszereinket átkonfiguráltuk, illetve bővitettük. Ennek során mindenütt realizáltuk a géptermek és környezetüknek a rendelet szellemének megfelelő átalakitását, illetve uj objektum esetében /pl. ÉGSZI-Szeged/ a legkorszerübb elvek alapján való kivitelezést.

E helyen is meg kell emlitenünk, hogy munkánkhoz a BM-TOP, illetve a helyi tüzoltó parancsnokságok és a tanácsok illetékes osztályai számottevő segitséget nyujtanak, hiszen egy telepitési elképzeléstől a használatba vételi engedély megszerzéséig sok a tennivaló. Nagyon fontosnak tartjuk, hogy a különféle veszélyhelyzetek feltárására és elháritására a

számitóközpontokat felkészitsük. Hangsulyozottan kiemeljük, hogy csak az utóbbi időszakban nyiltak meg a szélesebb lehetőségek arra, hogy a veszélyhelyzetek detektálására megfelelő automatikus elháritó rendszereket lehessen üzembe helyezni. E szempontból lényeges előrelépést jelent a SZOT Munkavédelmi Kutató Intézet és a GELKA tevékenysége, amelyek a tüz- és vagyonvédelem megfelelő eszközeit gyártó és azokat ellátó intézményekké nőtték ki magukat. A SZOT MTKI-val kialakitott kapcsolatunk lehetővé teszi, hogy az Intézet számitóközpontjainak automatikus vagyon- és tüzvédelmi rendszerét egységesitsük, jó ár/teljesitmény viszonyok mellett.

Az adatvédelmi és adatbiztositási feladatok között komoly szerepet kap a számitógép és környezetének őrzésvédelmi megszervezése.

Tervezés alatt áll - bázisintézeti feladatunkból adódóan -, hogy ágazati szintü referencia helyet alakitsunk ki e témakörben is. Elképzelésünk lényege, hogy a kijelölt számitógép-üzembe, illetve kitüntetett helyiségeibe a be- és kiléptetést mikroszámitógépre bizzuk.
Ennek segitségével a meghatározott be- és kilépési pontokat "programozottan" tudjuk ellenőrizni. /Zártláncu mágneskártyás ellenőrző rendszer./

A berendezés várhatóan a jövő év elején kerül installálásra.

Az Intézet az utóbbi időszakban jelentős összegeket áldozott a mágneses adathordozók klimatizált raktározási és szállitási kérdéseinek megoldására.

Ezen belül különös gondot forditottunk

- a master anyagok többszörös kópiáinak előirásszerü tárolására,

- a szállitás alkalmával előtérbe kerülő mechanikus védelemre és az átmágneseződés veszélyforrásainak kiküszöbölésére.

Előirtuk, hogy fontos információt tartalmazó adathordozó szállitása esetén

- a szállitás előtt másolat készitése kötelező,
- árnyékolást biztositó szállitóeszköz, illetve tárolódoboz alkalmazása szükséges.

A szállitmány elinditására, a szállitólevél aláirásával a küldő üzem vezetője, vagy helyettese jogosult. A szállitólevél csak akkor irható alá, ha a szállitás módja az előirásnak megfelel.

E fejezet végén szólunk néhány szót a rendkivüli események bekövetkezése esetén foganatositandó intézkedésekről, vagy más szóval a katasztrófatervről.
Ebben megfogalmaztuk, hogy a számitógéppel rendelkező főosztály vezetője - a helyi sajátosságok figyelembe vételével - intézkedési tervet köteles készitени, amely kötelező érvénnyel tartalmazza:

- a berendezések fizikai épségét és müködését veszélyeztető események felsorolását, ezen belül javaslatot tesz a megelőzésükre, leküzdésükre és a keletkező károk csökkentésére vonatkozó tervezetek kidolgozására,
- bekövetkezett zavarok, károsodások esetére szükséges riadóztatási terveket,
- a károk helyreállitására, valamint a keletkező kapacitáskiesések pótlására szolgáló javaslatokat.

Az emlitett intézkedési tervkoncepció kialakitásánál, illetve ajánlásánál mindenkor a célszerü munkamegosztás elvét

helyeztük előtérbe. Elvként rögzitettük, hogy a főosztályi szintü védelmi feladatokat - különös tekintettel a földrajzi tagoltságra - azokkal kell elvégeztetni és azok végrehajtásáért felelőssé tenni, akiknek munkakörében a védelmi feladat jelentkezik.

Dokumentálás, program-technikai eljárások

Dokumentálás

A számitógépes rendszerek biztonság-jóságánál ma már a dokumentálás az egyik fokmérő.
Nem kerülhetünk olyan helyzetbe, hogy egy kulcsfontosságu szakember távozása után, megfelelő dokumentálás hiányában rendszerünk müködtetését szüneteltessük.

E problémakör sulyával az Intézet évek óta tisztában van, ezért törekvésünk az átfogó, korszerü rendszerek fejlesztésének szervezeti, személyi és egyéb feltételeinek a mindenkori követelményekhez való igazitása. Az Intézet fejlesztő szervezetei - egyik alaptevékenységünknél fogva - az Ágazat és vállalatai számára információs igényüket kiszolgáló számitógépes programrendszereket készitenek, illetve a változásokhoz igazitják azokat.

Az elmult években megalapoztuk a regionális számitógép-hálózat mai és ujabb, nagyobb teljesitményü számitógépeinek hatékony felhasználását, folyamatosan alkalmazkodunk a müszaki-tudományos fejlődés követelményeihez. Ezek a feladatok megkövetelik, hogy végrehajtói következetesen tökéletesitsék módszereiket. Vonatkozik ez a dokumentációs rendszerre is, hiszen a rendszer-üzemeltetés és ellenőrzés nélkülözhetetlen kelléke a megfelelő dokumentálás.

Tekintettel arra, hogy az előadásban nemcsak pozitivumokat kivánunk bemutatni, gyakorlatunkból a számitógépes rendszerek dokumentálásával kapcsolatban két sarokpontot emlitünk meg:

- A nem kellő mértékü dokumentáltság és a hiányos dokumentáció a későbbiek során egy-egy rész ujratervezését, programozását igényelte, mivel nem volt kellő tájékozottság az adott időpontbeli állapotról;
- Eltulzott adminisztrativ jellegü, redundáns dokumentáció felesleges terhet rótt a rendszer karbantartójára és az üzemeltetőkre, igy bürokratikussá vált a dokumentálás, esetenként az érdemi müködési leirások helyett papirhalmaz került a doku-tárba, amelynek alkalmazhatósága és haszna erősen kétségbe vonható.

Miután több éves tapasztalatok azt mutatták, hogy az elmélet kiállta a gyakorlat próbáját, a megfelelő elemzések után még 1979-ben kidolgoztuk az Épitésügyi Szervezési és Program-Dokumentációk Egységes Rendszerét, amelynek célja az ágazati program-vagyon használatának könnyitése, uj elemei kidolgozásának egységessé tétele.

E szabványositási törekvés keretében rögzitettük a dokumentálás alapelveit, kölcsönhatását a számitógépes rendszerek fejlesztésével, valamint a kidolgozói, követési és felhasználói dokumentáció formai és tartalmi követelményeit.

A rendszerfejlesztés hatékonyságának növelése érdekében elkészitettük az állandóan bővithető un. ERPEL /Egységes Rendszertervezési és Programozási Elemek/ rendszert. Az ERPEL kész rendszertervi és programelemeket foglal magába, melyek a különböző szoftver termékekben változás nélkül felhasználhatók. Az ERPEL rendszer felhasználásának fókuszában a kód-

katalógus szigoruan determinált szabadságfoku felhasználása áll. Az emlitett adattár különböző felhasználói szoftver termékekbe történő egységes alkalmazása elsősorban egy-egy felhasználó vállalat információs rendszerének egységességét biztositja, illetve ez az egységes alkalmazás - a kódfelelősi funkciók centralizált ellátásán keresztül - egy-egy vállalatcsoportra, illetve népgazdasági ágazatra, alágazatra kiterjeszthető.

Az ERPEL rendszer szolgáltatásai a számvitel bizonylati rendjéről szóló 29/1978. /XI.14./ PM sz. és az ezt módositó 4/1982. /II.3./ PM sz. rendelet előirásainak betartását csaknem teljeskörüen biztositják.

Rendszerhasználati és -hozzáférési jogosultság

A számitógépes feldolgozások fejlődésével, azok rendszerekké kovácsolódásával ezek a kérdések valóságos védelmi problémává váltak, ezen tulmenően az adatbázisok használatának és a távadatfeldolgozás alkalmazásának szélesedésével nemcsak probléma, hanem gond is lett.

Közismert, hogy minél nagyobb biztonságot kivánunk elérni a rendszerhasználati és adathozzáférési jog ellenőrzésénél, az annál nagyobb tehet ró a feldolgozó rendszerre. A védelem e formájának sarkalatos pontja, hogy a programozott adatvédelmi megoldások szükebb értelemben a feldolgozás hatékonyságát rontják. A védelem szervezésének egyik kulcskérdése az adminisztrativ és gépi ellenőrzés optimalizálása.
Munkánkban általános elvnek tekintjük, hogy a védelem mértékének a védelem tárgyával mindenkor arányban kell lennie, bármilyen eltérés problémák forrása lehet.
Az integrált adatbázisok, továbbá ezek távadatfeldolgozása, kezelése a szoftver szállitó cégeket védelmet biztositó eljárások kidolgozására készteti.

Ezek azonban általános jellegü megoldások és nem minden esetben nyujtják az előirt védelmi komfortot.
Az Intézetünk által használt különböző operációs rendszerek eltérő mértékben nyujtanak védelmet és biztonságot.
Ahol az operációs rendszer csak kismértékben támogatja a téves, vagy rosszhiszemü felhasználás elleni védekezést, ott célraorientált védelmi modulok kifejlesztésében jelennek meg a biztonságra való törekvéseink, illetve a megfelelő szoftver eljárások az adat speciális kódolására épülhetnek. Kidolgozásuk és a beépitési pontok meghatározása programcsomagonkénti tervezési feladat. A fejlettebb operációs rendszerek esetében /DOS/VS, OS, BS 2000/ jobban támaszkodunk az üzemrendszer által nyujtott szolgáltatásokra, és a védelmi rendszer részeit beépitjük az operációs rendszer szolgáltatásai közé.

A korábbiakban már emlitésre került, hogy többféle operációs rendszerrel foglalkozunk, ezek közül értékelünk néhányat az adatvédelem lehetőségeinek tükrében.

DOS:

Ebben az operációs rendszerben a cimke kezelés az egyetlen olyan védelmi lehetőség, amely a szándékos adatsértést és adatleolvasást megakadályozhatja. A szándékosságot erősen hangsulyozni kell, hiszen az operátor engedélyével ugy a megőrzési idő, mint a nem használt állományok egyszerüen felülirhatók.
Mágneses állományok esetén még cimke egyezés sem szükséges ahhoz, hogy az operátor engedélyezze az állományok használatát irásra vagy olvasásra.
Mágneslemezeknél pedig az állományok nevét ugyan pontosan kell tudni, de ehhez az információhoz bárki hozzájuthat egy cimke kiirással.

Az előbbiekből látható, hogy ezek a körülmények még a véletlen felülirás ellen sem biztositanak, hiszen egy operátori tévedés adatállományt szüntethet meg.
Az utóbbinál valamit javit a helyzeten, hogy a felülirás DSF/data secured file/ opció használatával megakadályozható. Ilyen környezetben a hozzáférés jogosságának kérdéseit elsősorban üzemeltetési előirásokkal tudjuk biztositani.

DOS/VS:

A DOS/VS rendszert kötegelt és interaktiv /ETSS/ üzemmódban használjuk. Ennek megfelelően az adatvédelem lehetőségeit is ketté kell választani.

Kötegelt /BATCH/ üzemmódban olyan illetéktelen, akinek nincs érvényes jobneve és témaszáma, nem dolgozhat.
Aki viszont illetékes a rendszerben való munkára, az elvileg az általánosan használt segédprogramok alkalmazásával minden információhoz hozzájuthat.

Interaktiv üzemben csak az dolgozhat, akinek érvényes LOGON neve van, ismeri a hozzátartozó jelszót és az ÉGSZI LOGON eljárása az illető nevét is ellenőrzi.

Az ETSS membereket azok tulajdonosa külön jelszóval is védheti /ez a jelszó nem feltétlenül azonos a LONGON-hoz tartozó jelszóval és meglehetősen szabadon választható, akár memberenként különböző is lehet/.

A fentiek alapján elmondhatjuk, hogy a DOS/VS ETSS üzemmódban az adatok véletlen megsemmisitése, vagy meghamisitása ellen védelmet nyujt, és alkalmat ad a szándékosság elleni védelemre is.

Véleményünk szerint néhány egyszerü adminisztrativ intézkedés betartásával kiegészitve az emlitett üzemmód alapvédelmi fokozattal minősitett titkok védelmét biztosithatja.

OS:

Az általunk használt OS verzióban a belépéshez szükséges egy munkaazonositási szám ismerete, amelyet a HASP JOB kártya számlázási információ mezőjébe kell megadni. A hibás azonositóval rendelkező JOB-ok a beolvasás után törlődnek, tehát illetéktelen személyek által leadott feladatok nem futhatnak.
Az OS rendszerben az adatállományok elérése a nevükön keresztül történik, melyet a JOB vezérlőnyelv /JCL/ segitségével kell megadni. Cimkézetlen mágnesszalagon elhelyezkedő adatállományok esetén meg kell adni a cimkében elhelyezkedő nevet.
A feldolgozás a cimkében szereplő név és a JCL-ben megadott név egyezősége esetén lehetséges.
Továbbá védelmi lehetőség a megőrzési idő használata.
A különböző háttértárakon tárolt adatállományok védhetők a létrehozásukkor megadott jelszó segitségével is.
Ha a jelszó definiálása megtörtént, minden egyes eléréskor ellenőrzésre kerül az elérés tipusa.
Ha az elérés és a jelszó tipusa megegyezik, az I/O supervisor az operátortól bekéri a jelszót.
Az állomány elérése csak az operátortól kapott pontos válasz után lehetséges.
Az emlitett pozitiv védelmi lehetőségek ellenére mélyebb OS ismeret birtokában /pl. system manager/ bármely adatállomány elérhető.

BS 2000:

A felhasználó csak akkor tud pl. terminálról egy folyamatot létrehozni, azaz a rendszert használni, ha a rendszerrel közli a felhasználói azonositót, a számlaszámot és a jelszót.

Felhasználói azonosító:

Kötelező, az alapszoftver ellenőrzi.

Maximum 8 karakteres alfanumerikus érték, a rendszer-karbantartó hozza létre, csak ő törölheti, vagy zárhatja ki ideiglenesen.

Számlaszám:

Üzemeltetési előirás szerint kötelező és egy vagy több, maximum 8 karakteres számlaszám tartozhat egy felhasználói azonositóhoz.
Csak a rendszer-karbantartó hozhatja létre, vagy törölheti.

A felhasználó csak az azonositója alatt létrehozott folyamatban kérdezheti le a saját azonositójához tartozó számlaszámait.

Jelszó:

Felhasználói kérésre a rendszer-karbantartó hozhatja létre. Egy felhasználói azonositóhoz max. 4 byte-os, karakteres, vagy hexadecimális értékkel.

A BS 2000 operációs rendszer - a részletek ismertetésétől ezuttal eltekintve - számos olyan "trükköt" ismer, amely szoftver oldalról kielégiti a fokozott biztonsági kategória követelményeit.

Az általunk használt további operációs rendszerek adatvédelmi szempontból történő vizsgálatával ez alkalommal nem foglalkozunk. Megemlitjük, hogy elsősorban az osztott információ rendszerek kialakitásának időszerüsége miatt megoldottuk a kisebb gépek /SZM-4/ adatvédelmének alapvető problémáit, illetve dolgozunk azok folyamatos kibővitésén.

Program-technikai eljárások

Az előzőekben adatvédelmi oldalról közelitve áttekintettünk néhány operációs rendszert.
A továbbiakban elsősorban azokról a megoldásokról beszélünk, melyeket az alkalmazói programokba épitettünk be, illetve melyek felhasználásával módositottuk az üzemrendszereket.

Mint már emlitettük, a programtechnikai védelmi eszközök kötegelt feldolgozási környezetben viszonylag szük lehetőséget biztositanak. Különösen elmondható ez az illetéktelen használat elleni védekezés módjaira, hiszen itt az adott termék /program, adattár/ fizikailag is kikerül az illetékes számitóközpont területéről, ezáltal lehetővé válik a védelmi eszközök módszeres felderitése.

A programtechnikai védelmi eszközök alkalmazásának célja kettős:
- megakadályozni a véletlen - gondatlan - károkozást,
- megnehezíteni a szándékos károkozást: az Intézet szellemi tulajdonát képező termékek illetéktelen felhasználását.

A véletlen - gondatlan - károkozás kategóriájába sorolhatók az adattárak téves felhasználása és az adattárak üzemeltetési hiba miatti megsérülése.

Az adattárak téves felhasználása akkor következik be, ha egy meghatározott adattár helyett egy vele formailag azonos felépitésü másik adattárat alkalmazunk. Az ekkor kapott eredmények hamisak lesznek. Ha ezt időben felfedezzük, akkor jó esetben csak a feldolgozás költsége jelent kidobott ráforditást. Előfordulhat azonban, hogy az adattárcsere csak alaposabb elemzéssel állapitható meg, akkor az adatok felhasználása további közvetett károkat okozhat. Az Intézetben

a téves felhasználás lehetősége elvileg és gyakorlatilag is fennáll. Területi számitóközpontjaink számos felhasználó számára futtatják ugyanazt a rendszert, körülbelül azonos időben. Hasonló probléma vetődik fel néhány központi adattárnál, ahol az adattár több változata áll rendelkezésre, és a feldolgozást egy meghatározott változattal kell elvégezni.

Az üzemeltetési hiba miatti adattársérülés /adattár felülirása, bizonyos rekordok, vagy kötetek logikai megsemmisülése/ általában jól észlelhető, azonnal kiderithető hibát okoz a feldolgozás során. Itt közvetlen kárként tehát csak a feldolgozás költsége jelentkezik. Nehézség akkor merül fel, ha a sérült adattár nem állitható helyre. Itt még a gondos mentés sem segit mindig. Előfordulhat olyan eset, hogy szoftver vagy hardver hiba miatt egy közvetlen hozzáférésü állomány - bizonyos - ritkán használt rekordjai iródnak felül, igy a hiba többszöri mentési cikluson keresztül is megmarad, amikor az eredeti állomány már nem áll rendelkezésre.
A téves használat, illetve az üzemeltetési hiba miatti sérülések kivédésének módjai hasonlóak: a lehető legnagyobb biztonsággal be kell azonositani az adatállományt, továbbá a feldolgozások során meg kell győződni az adatállomány logikai sértetlenségéről. Ennek érdekében az operációs rendszer biztositotta állomány azonositáson tul széleskörüen alkalmazzuk az adatállományok egyedi cimkékkel történő azonositását, a cimkék ellenőrzését megadott paraméterek alapján. Az un. vállalatrekordok vagy adminisztrációs rekordok rögzitik az adott állomány tulajdonosát, a feldolgozás jellemzőit /az állomány generáció-verzióazonositóját, a létrehozás dátumát, a feldolgozó program nevét, a feldolgozás időpontját, jellegét stb./. Az állományok ilyen jellegü azonositása az Intézetben teljeskörü. Az azonositás megkönnyitése érdekében általános eljárásokat készitettünk, melyek lehetővé teszik a

programozó számára az egyébként általában nagy programozásigényü azonositások egyszerü elvégzését, és ezáltal garantálják az azonos szerkezetü vállalatrekordok kialakitását.

Néhány programcsomagban adminisztrációs állományokat hoztunk létre. Ezek az állományok regisztrálják a programcsomaggal végzett összes feldolgozást, az egyes adattárak állapotát. Az adminisztrációs állományokat futtatásszervezésre is felhasználjuk, ezáltal csökkentve a feldolgozási hibák valószinüségét.

Számos programból álló, összetett rendszereknél sikerrel alkalmazzuk a JSERV futtatásszervező rendszert, amely biztositja a futtatások automatizmusát, csökkentve ezáltal a hibák lehetőségét.

Általános eljárást dolgoztunk ki a jobok közötti kommunikációra, ez lehetővé teszi az olyan hibák megakadályozását, ami az egyes programok várható meghibásodásából származik.

A téves felhasználás, meghibásodás elleni védelem céljára a programokba beépitett kód mennyisége a programcsomagok 15-30 százalékát teszi ki. Ebben természetesen nemcsak az itt felsorolt megoldások találhatók, hanem a paraméterezés, paraméterellenőrzés, listák készitése a futási eseményekről, rekord és tételszámlálások, a rendeletek szerinti kötelező azonositások stb. megirásához szükséges kód is. Mindezek együttesen szolgálják az adatállományok védelmét, a gazdaságos, hibamentes feldolgozást. Ugyanakkor ezek a megoldások jelentős fejlesztői kapacitást kötnek le, és az egyes rendszerekben alkalmazott eltérő védelmi módszerek nehezitik a futtatásszervezést, növelik a feldolgozások idejét.

Céljaink között szerepel tehát a közeljövőben az ilyen jellegü védelmi megoldások egységesitése, és további olyan megoldások kialakitása, amelyek általánosan alkalmazhatók a téves használat, illetve üzemeltetési hiba megakadályozására, az ebből eredő feldolgozás ismétlések számának csökkentésére.

Mig a véletlen hibák esetében az ezt kivédő megoldások egységesitésére törekszünk, a szándékos eltulajdonitás elleni védelem esetében - értelemszerüen - minél változatosabb megoldásokat keresünk.
Az adattárak illetéktelen felhasználása elleni védekezés - ha az fizikailag kikerül a számitóközpont területéről - meglehetősen nehéz, de van rá mód. Speciális kódrendszerek alkalmazására csak néhány, különösen fontos adattár esetében vállalkozhatunk, mivel ezek alkalmazása jelentősen növeli a feldolgozási időt /programtechnikai megoldásokról van szó/.

A programok illetéktelen használatának megakadályozására kialakult megoldásaink vannak, ezek közül ismertetünk egyet.

A védelmi modul, mint felhasználói adatvédelmi szoftver

A programok illetéktelen használatának módozatai két kategóriába sorolhatók:

- adott időpontban jogcim nélkül történő használatra, és
- adott helyen jogcim nélkül történő használatra.

Az első esetben a program futtatása olyan időszakban történik, amelyre az alkalmazónak és a forgalmazónak nincs érvényes szerződése, azaz nem kötöttek adás-vételi szerződést, ill. a bérleti szerződés lejárt.
A második esetben a programot más hardver-szoftver környezetben kivánják futtatni, mint amelyikre az adás-vételi vagy bérleti szerződés szólt.

Mindkét esetre kidolgozható olyan számitástechnikai módszer, amely

- segiti a forgalmazó érdekeit sértő esetek mielőbbi felderitését és
- biztositja, hogy a jogtalan használat tárgya müködtethetetlen, vagy nehezen müködtethető legyen.

Azokat a programokat, alprogramokat vagy programrészeket, amelyek azzal a céllal készülnek, hogy az emlitett két feladatot egy szoftver-termék számára ellássák a továbbiakban védelmi modulnak nevezzük. Az elnevezést függetlenül használjuk attól, hogy programozási értelemben önálló modulként, vagy esetleg csak több helyen szereplő programrészként valósul meg.

A védelmi modullal szemben a következő követelményeket támasztottuk

a./ Korrektség:

A modul nem gyakorolhat büntetőszankciót semmilyen más számitástechnikai termékre. Nem ronthat el más programokat vagy adatállományokat, miközben saját illetéktelen müködtetését igyekszik megakadályozni. Ha egy programfuttatást vagy feldolgozási folyamatot meghiusit, azt ugy kell tennie, hogy a felhasználó számára egyértelmü legyen az esetleges outputok használhatatlansága.

b./ Rejtettség:

A modul fizikai helyének és müködési elvének a mindenkori alkalmazók előtt ismeretlennek kell maradnia. Lehetőség szerint neheziteni kell a felismert védelmi modul kiiktatására irányuló felhasználói törekvéseket.

c./ Gazdaságosság:

Az előző két feltételt ugy kell kielégiteni, hogy
- a védelmi modul teljes kifejlesztési költsége az egész programtermék fejlesztési költségéhez képest alacsony legyen,
- a modul üzemeltetése a programtermék üzemeltetési költségeit jelentősen ne emelje.

A védelmi modul müködtetésének feltételei

Egy adott időpontban történő jogcim nélküli használat megakadályozásának feltétele, hogy a védelmi modul a napi dátumot ismerje, arról megfelelő gyakorisággal tájékozódni tudjon. Amennyiben az alapszoftver környezet ezt támogatja, megvalósitása nem okoz különösebb gondot.
Ellenkező esetben is találhatók áthidaló megoldások: például a programrendszer maga szervez ilyen célu dialógust a táblákra irandó napi dátum ürügyén.
A jogcim nélküli helyen való felhasználás felderitéséhez a védelmi modulnak ismernie kell a szoftver környezet néhány, a felhasználásra nézve jellegzetes, egyedi tulajdonságát az installálás időszakában. Ilyenek lehetnek pl. az input-output készülékek kezelését biztositó felügyelő program adminisztrációs tábláinak tartalma, a tárméret, bizonyos állandóan a tárban tartózkodó szoftver komponensek kezdőcime, esetleg azok azonositója stb.

Természetesen tökéletesen azonos hardver és szoftver feltételek mellett a védelmi modul nem tud jogos vagy jogtalan használat között különbséget tenni.

Ha egy jogos alkalmazó akar a forgalmazóval való szerződést nem érintő olyan hardver, vagy szoftver fejlesztést végrehajtani, amely a védelmi modul által figyelt paramétereket módositaná, akkor a modul a futtatást ugyanigy meghiusitja

/pl. valamilyen programhiba megszakitással/ mintha jogcim nélküli használat történt volna. Ilyenkor a forgalmazó garanciális javitási kötelezettségének eleget téve a "programhibát" kijavitja, azaz a védelmi paramétereket a fejlesztést figyelembe véve korrigálja.

Célszerü, ha az adás-vételi, ill. bérleti szerződések eleve tartalmaznak utalást arra, hogy a konfiguráció módositását, az operációs rendszer verzió váltását, vagy ujragenerálását az alkalmazó fél a forgalmazónak bejelenti.

A védelmi modulok készitésének és karbantartásának feltételei

A védelmi modulok tervezése és kivitelezése átlagon felüli szakmai intelligenciát és jártasságot igényel. Egyszerre kell áttekinteni egy nagyobb számitástechnikai rendszert és a fogadó gép alapszoftverjének specifikumait. Több programnyelv ismeretét követeli meg.

Biztositani kell a védelmi modulok teljeskörü dokumentáltságát, természetesen a titkos ügyiratkezelés szabályainak betartása mellett.

Meg kell oldani, hogy a feladattal több, egymást konkrét esetekben helyettesiteni tudó munkatárs foglalkozzon, akik lehetőleg azonos szervezeti egységhez tartoznak.

Összefoglalva: tapasztalataink azt mutatják, hogy a védelmi eszközök alkalmazásának nem lehet célja az adattárak, illetve a programok abszolut védelme, a programtechnikai eszközöket megfelelő szervezési, adminisztrativ szabályozással, rendszeres ellenőrzéssel együttesen kell alkalmazni.

Dr. Borda József:

SZÁMITÓGÉPES RENDSZEREK BIZTONSÁGI KÉRDÉSEI

Napjainkban a számitógépes információs rendszerben a vállalatok létfontosságu információinak többsége összpontosul. Igy ezek védelme, biztositása a vállalatvezetők fontos feladata. Az adatfeldolgozás szélesebb körü alkalmazásával, fontosságának növekedésével a fel nem deritett hibákból és kihagyásokból származó veszteség lehetősége is megnövekedett. Hibalehetőségek állnak fenn a számitógépes alkalmazási rendszerek, a számitóközponti tevékenységek és az alkalmazási rendszerek fejlesztése területén. Az adatfeldolgozás hosszabb ideig tartó kimaradása sok szervezet folyamatos működése szempontjából katasztrófális következményekkel járhat. Igy érthető, hogy a számitástechnika fejlődésével fokozott érdeklődés tapasztalható annak biztonsági kérdései iránt is. Az utóbbi 10-15 évben nagy számban fordultak elő - elsősorban a nyugati országokban - számitógépes bünesetek, visszaélések, s a felhasználók részéről gyakori volt az elégedetlenség az információk pontosságával kapcsolatban.

A védelmi eszközök kiválasztásához, bevezetéséhez ismerni kell azokat a tipikus hibákat és veszélyhelyzeteket, amelyekkel a számitástechnika alkalmazása során számolni kell. Bármely rendszeren belül a hibaforrások helyes megitélése az előfeltétele annak, hogy ezek lehetséges hatását, s kiküszöbölésük módját vizsgálhassuk.

Az adatok pontosságát veszélyeztető hibák elleni védekezésnek viszonylag kialakultak már a módszerei. A szándékos veszélyeztetés, az illetéktelen információszerzés megelőzésére alkalmas módszerek - mivel e jelenségek viszonylag ujkeletüek a számitástechnikában - alkalmazására még a kisérletezés, tapasztalatszerzés a jellemző.

Az adatfeldolgozás hibalehetőségei

A témával nagyon sok szakkönyv foglalkozik és sok szerző rámutat azokra a fenyegetésekre, hibalehetőségekre, amelyek az adatfeldolgozási rendszerekkel kapcsolatban előfordulhatnak.

Hatékony ellenőrzési, biztonsági rendszer kiépitése csak a már előfordult hibák, visszaélések alapos elemzésével vagy a számitástechnikai folyamatok "gyenge" pontjainak elemzésével képzelhető el.
Többen különbséget tesznek a véletlen vagy önkényesen kezdeményezett információ felfedések között. Az utóbbinál gyakran különbséget tesznek passziv és aktiv módszerek között.
Passziv módszernek nevezik a lehallgatást, aktivnak minden olyan a normál hozzáférési eljárástól eltérő müveletet, amit az illetéktelen felhasználó végez, hogy adatokhoz jusson hozzá.
Fontos megjegyezni, hogy a legtöbb szerző véleménye megegyezik a kezelő személyzet megbizhatóságának fontosságában. A kezelő személyzet megbizhatatlansága esetén a rendszert az ilyen fenyegetésekkel szemben rendkivül nehéz megvédeni.

A szakirodalomban ugyan számos hibatipus szerinti osztályozás található, de ezek hiányossága, hogy általában nem a megelőzésükre, felfedezésükre s javitásukra vonatkozó ellenőrzési, biztonsági intézkedések figyelembe vételével történtek.

A SZÁMALK Oktatási Iroda gyakorlatában a következő csoportositási elvet alkalmazzuk a hibák és veszélyhelyzetek elemzésénél:

- a számitóközpont környezetében és az üzemeltetés során előforduló hibák, veszélyforrások, amelyek nem egy, hanem több alkalmazásnál is éreztetik hatásukat;

- a rendszerfejlesztés során előforduló hibák;
- az egyedi alkalmazási rendszerek tipikus hibái.

A számitóközpont környezetében és az üzemeltetés során előforduló veszélyforrások pl.

- A számitóközpontban a munka és felelősségi körök helytelen kialakitása,
- Véletlen adattörlés adathordozóról,
- A file-könyvtár helytelen kezelése, könyvtárosi funkció kialakitásának mellőzése,
- Operátori hibák, üzemeltetési dokumentáció karbantartásának elmulasztása,
- Adatelőkészitési, rögzitési hibák,
- Rossz file és program alkalmazása,
- Programok kipróbálásának, tesztelésének hibái,
- Adathordozók elvesztése, helytelen tárolása, elkeveredése, gondatlan selejtezése,
- Outputok helytelen tárolása,
- Alapsoftware hibák, a software-t nem látják el a különböző biztonsági igényeket kielégitő védelmi rendszerrel,
- Müszaki hiba /vonalhiba, generátor stb./,
- Hardware védelmi eszközök meghibásodása.

A rendszerfejlesztés során előforduló tipikus hibák pl.

- A rendszerterv nem a felhasználók igényei alapján készül,
- A rendszerterv specifikációs része hibás vagy hiányos,
- Rendszerterv nem a rendelkezésre álló hardware és software lehetőségekre épit,

- Rendszerterv hiányos a kivitelezési szakasz elvégzéséhez,
- Nincs ellenőrző pont a rendszerben a hibás munka korrigálására vagy a projekt megszüntetésére,
- A rendszer folyamatos karbantartási igényeit figyelmen kivül hagyják.

Az alkalmazási rendszerek tipikus hibái pl.

Az inputtal kapcsolatos hibák: az input elveszik, duplikálják az inputot, tartalma pontatlan, adat hiányzik, nem rögzitik a tranzakciót stb.

A feldolgozásnál előforduló hibák: a feldolgozás során rossz file-t használnak, a tranzakciókat rossz rekorddal dolgozzák fel, a feldolgozás nem teljes vagy pontatlan, a változó körülményekhez rugalmatlan a feldolgozás, file-ok, programok elvesztése stb.

Az outputra jellemző hibák: az output szétosztása nem megfelelő, későn jut el a cimzetthez, vagy elveszik, nyilvánvalóan hibás,
hibás, de a plauzibilitási határokon belül, nagyszámu hiba kijavitására nincs lehetőség az adott határidőn belül,
az output pontosságának a bizonyitására nem állnak rendelkezésre bizonyitékok stb.,
James Martin a "Security, Accuracy and Privacy in Computer Systems" cimü müvében nem csupán a veszélyeket ismerteti, hanem a lehetséges következményeket is vizsgálja.
A következő táblázat is bizonyitja, hogy James Martin módszerét alkalmazva hasznos kockázatelemezési segédeszközt fejleszthetünk ki.

VESZÉLYFORRÁSOK	Működésképtelenség	Teljes file elvesztése	Egyedi rekordok elvesztése	Rekordok módosulása	Jogosulatlan olvasás vagy kiírás
Rosszindulatu károkozás					
rablás	x	x			
erőszakos szabotázs	x	x			
nem erőszakos szabotázs /pl. szalag törlése/	x	x	x	x	
rosszindulatu számitógép operátor		x	x	x	
rosszindulatu szalagkönyvtáros		x			
rosszindulatu terminálkezelő		x	x	x	
rosszindulatu alkalmazó /pl. olyan alkalmazó, aki lyukakat lyukaszt visszatérő kártyákra/			x	x	
Emberi gondatlanság					
lyukasztási hiba			x	x	
terminálkezelő input hibája			x	x	
számitógép operátor hibája		x	x	x	
nem megfelelő szalagot vagy lemezcsomagot rakták fel és tartották karban		x		x	
nem megfelelő programverziót alkalmaztak		x		x	
rossz program tesztelés		x	x	x	
lemezt vagy szalagot nem megfelelően rakták fel		x			
a szalag vagy lemez fizikai sérülése		x	x		
Bünözés					
hütlen kezelés			x	x	x

VESZÉLYFORRÁSOK	Működésképtelenség	Teljes file elvesztése	Egyedi rekordok elvesztése	Rekordok módosulása	Jogosulatlan olvasás vagy kiírás
ipari kémkedés					x
alkalmazottak eladnak kereskedelmi titkokat					x
alkalmazottak eladnak címlistát					x
adatbank információ felhasználása megvesztegetés céljára					x
Mechanikai hiba					
számítógép meghibásodása	x				
file-egység megrongálja a lemezsávot			x		
szalagegység rongálja a szalag egy részét			x		
lemez vagy más adathordozó olvashatatlan		x			
hardware vagy software hiba rongálja a file-t		x	x	x	
fel nem fedezett adatátviteli hiba			x	x	
a kártyát /vagy más inputot/ rongálja a gép			x	x	
az alkalmazói program hibája rongálja a rekordot			x	x	

A számítógépes bünözés

A számítógépes bünözés fogalmát még a szakemberek is vitatják. Értelmezésünk szerint a számítógépes bünözés fogalmába tartozik minden olyan jogtalan, szándékos cselekedet, amelynek elkövetéséhez számitástechnikai ismeret szükséges,

amelyet számitógépes adatfeldolgozási eszközzel követnek el, vagy amelynek célja éppen a számitógépes adatfeldolgozási eszközök megrongálása, az azokban való károkozás.
A feltárt és közölt számitógépes visszaélések ma a világon az elkövetett eseteknek csak kis hányadát jelentik. Nagyon sok intézet ugyanis presztizs okok miatt nem tárta nyilvánosság elé az ügyet. Donn B. Parker egyik müvében részletesen elemzett 669 számitógépes visszaélést. Elemzésében feltárta az okokat, a visszaélés tipusát, s néhány esetben az okozott kárt. A 669 számitógépes visszaélés az elkövetés tipusa szerinti csoportositását a következő táblázat mutatja be.

Az ismert számitógépes visszaélések csoportositása

Visszaélés tipusa	száma
Fizikai megsemmisités	97
Információ lopás	185
Pénzügyi csalás	284
Szolgáltatások jogosulatlan igénybevétele	103
Összesen:	669

A visszaélések elemzése alapján megállapitható, hogy a számitógépek alkalmazásával nem merültek fel uj inditéku büncselekmények, de a számitógép alkalmazása megváltoztatja a módszert, változik a visszaélők szolgálati beosztása és változik a veszélyeztetett értékek tipusa. A vandalizmus, az információlopás, a pénzügyi visszaélés, a szolgáltatások jogosulatlan igénybevétele olyan kategóriákat jelentenek, amelyek mindenütt előfordulhatnak. Ujszerü és a közvélemény érdeklődését nagymértékben kiváltó ok az volt, hogy ezek számitógépes környezetben is lehetségesek, felfedésük uj speci-

ális ismeretanyagot kiván.

A számitógépes visszaélések elemzése alapján megállapitható, hogy a számitógép négyféle szerepet tölthet be a visszaélés során. Lehet a támadás célja, eszköze, környezete, s a számitógépet mint szimbólumot is felhasználhatják.

A számitógép a visszaélés célja és tárgya a következő esetekben:

- a számitógép ellopása,
- szolgáltatások jogosulatlan használata,
- vandalizmus a rendszer ellen,
- az adatok megsemmisitése,
- hibás müködés előidézése,
- a számitóközpont alkalmazottai "saját zsebre" eladják a gépidőt, vagy szolgáltatásokat vesznek igénybe.

A számitógép akkor a visszaélés eszköze, ha alkalmazását használják fel a visszaélés elkövetésére.
Előfordult, hogy a számitógépet csak szimulációra, s nem közvetlenül használták fel a visszaélés során.

A számitógép környezetet jelent a visszaélés számára, ha a rendszerből lehetővé válik a programok és adatok ellopása. A mágneses adathordozókon tárolt programok és adatok olyan uj értéket jelentenek, amelyhez gyakran próbálnak illetéktelenül hozzájutni.
A számitógépre hivatkozva félrevezethetik a közvéleményt, amikor például a szándékosan vagy véletlenül elkövetett emberi hibákat a számitógép hibájaként tüntetik fel.

Kétségtelen, hogy a számitógépet üzemeltető szervezetek többségénél tudatosság tapasztalható az adatfeldolgozás hibalehetőségeit, veszélyforrásait illetően. Tapasztalható azonban olyan jelenség is, hogy a felső vezetőket nem tá-

jékoztatják a konkrétan előfordult hibákról, amelynek esetleg komoly anyagi következménye is van. Véleményünk szerint ez inkább a tájékoztatás hiányosságaira vezethető vissza, mintsem arra, hogy nálunk nem aktuális az adatfeldolgozás felsorolt hibalehetőségeivel foglalkozni. Az a törekvés, hogy a hibákat "ameddig lehet elkendőzzük" általánosnak tekinthető. Pl. 2000 - zömében amerikai és nyugat-európai - intézményeknél végzett felmérés során a válaszadó felső vezetőknek csak 17 %-a vallotta, hogy az adatfeldolgozás hibáiról rendszeres jelentéskötelezettség van a szervezetüknél. Valójában nem találtak olyan intézményt, amely megbizható módszerekkel rendelkezett volna a potenciális veszteségek mérésére.

Gyimesi László:

A FELHASZNÁLÓI KÖRNYEZET ÉS A SZÁMITÓGÉPES RENDSZER BIZTONSÁGÁNAK NÉHÁNY KÉRDÉSE

/KORREFERÁTUM/

A rendszerek müködésének hétköznapjairól szólnék, azokról az eseményekről, amelyek a rendszerek üzeme során történnek. Ismertetném az adatgyüjtés és a feldolgozás általam használatos módszerét és utalnák az adataival elvégzett elemzések eredményeire. Befejezésképpen az eredményadatok birtokában a rendszertervezés egyes lépéseinek a fontosságára hivnám fel a figyelmet. Ezen belül a feldolgozásokba épithető ellenőrzési eljárások szükségességére, amelyek a rendszerek biztonságát lényegesen növelhetik.
Előadásom nem titkolt célja az, hogy a feldolgozások müködéséért felelős kollegáimat arra késztessem, hogy értékeljék, elemezzék az irányitásukkal létrehozott rendszereket, okuljunk az elkövetett hiányosságokból.

A számitógépes rendszerek tervezése, a tervezés irányitása a kész rendszerek használatbavétele, az üzemeltetés munkája során a szakembereknek nap mint nap szembe kell nézni a siker, vagy a kudarc tényével. Foglalkoztatott a probléma és elkezdtem kutatni, milyen megoldásokkal találkozhatunk a sikeresnek, biztonságosnak mondott rendszerek esetén, valamint mi az oka annak, hogy egyes rendszerek soha nem érik el az elvárt müködés szintjét. Ahhoz, hogy a rendszer belső összefüggéseit feltárhassam, előbb a jelenségeket kellett részletesen megfigyelnem. A történésekről információkat kellett szereznem. Első közelitésben a kudarc okait vizsgáltam. Az adatgyüjtés során több forrásra támaszkodtam. Az első adatforrást a hivatalos, a legtöbb számitóközpontban meglévő és vezetett hibajelentők adatai képezte. A második

adatforrást azok az információk jelentették, amelyeket a termelési tárgyu vezetői megbeszéléseken szereztem. A harmadik adatforrást a saját un. nyomozómunka eredményeképpen nyert információk képezték. A rendszerek komplexitása alapján ugy gondolom, hogy minimálisan-hasonló vizsgálat elvégzéséhez az előbb elmondott hármas adatgyüjtésre van szükség. A rendszerelemek közti kapcsolatok feltárása olyan információkat igényel, amelyekkel a számitógépes üzemeltetés folyamatában résztvevő szakemberek közül egymaga senki nem rendelkezik. A szervezeti felépitésből adódó elszigeteltség olyan mértékü, hogy a rendszerüzemeltetésről, a rendszerben lejátszódó folyamatokról, a felhasználóra gyakorolt hatásáról csak részleges információk képződnek egyes munkahelyeken, és rendszerhiba esetén a megitélések erősen a szervezeti hovatartozás szerint polarizálódnak.

Ezzel a véleményemmel nem a jelenlegi üzemeltetési szokások és a számitóközpontok szervezeti felépitését kivánom birálni, hanem arra a tényre utalnák, hogy az egycsatornás adatgyüjtésre támaszkodó hibamegállapitás milyen veszélyt rejt magában és hogy az igy nyert adatok kiegészitése mindenképpen szükséges.

Elemzésem tárgyát a rendszerek hibás müködéséről nyert adatok képezik. Egy-egy hibás rendszer müködéséről az alábbi információk álltak rendelkezésemre:

- a munka azonositója, vagy munkaszáma,
- a számitógép tipusa, megjelölve azt, hogy milyen operációs rendszer alatt történik az üzemeltetés, a rendszer futtatása,
- a feldolgozás időszaka, havi részletezettséggel,

- az anyag jellege, ami a felhasználói rendszerek csoportokba történő sorolását jelenti,
- a rendszerek futtatásának gyakorisága,
- a hiba tipusa,
- az ujra futtatás során felmerülő költség mértéke, a kár összege,
- az anyag felelősének a kódja,
- egy kód arra vonatkozóan, hogy a rendszerhiba okozott-e kárt a felhasználónál, vagy sem,
- és végül egy kód értéke utal arra, hogy a hiba elemzése során nyertem-e olyan információt, amely segitséget nyujtott a ténylegesen történtek megállapitásához.

Az elemzéshez 114 rendszer meghibásodás - az előbb felsorolt adatai - képezték az alapot.

Mielőtt az elemzés módszerét ismertetném a kapott eredmények birtokában visszautalnák az adatgyüjtés tartalmához. Részletesebb eredményt kapunk, ha a gyüjtendő adatok közé felvesszük a rendszer készitőinek adatait, a rendszer készitésének, módositásának dátumát, a müszakszámot, /amikor a hiba előfordult/ a keletkezett károsszeget tovább bontjuk, a gépidő igényt, a papirfelhasználást, a szükséges szellemi ráforditást természetes mértékegységükben is feltüntetjük. Segiti az elemző munkát ha az adatok felvétele során a hiba kódolását aszerint is elvégezzük, hogy a tervezés munkafázisának melyik szakaszába tartozó ellenőrzési megoldás hiánya okozta a problémát. Természetesen ezen mintavétel csekély számu adatainak feldolgozása nem képzelhető el a számitógép igénybevétele nélkül.

A kigyüjtött adatok csoportositásához az egyes adatok közti összefüggések megállapitásához többszöri futtatásra van szükség, hiszen csak igy fedhetők fel az adatok közti összefüggések és kerülhetők el a téves megállapitások. Ennek elvégzése nem okozott számomra gondot, mivel lehetőségem volt az elemzést matematikai-statisztikai programcsomag felhasználásával elvégezni. Megjegyzem, hogy az adatelőkészités és a programok lefuttatása csak minimális időt vett igénybe. Az adatok bevitele előtt a hibáknak és az anyagcsoportoknak a kódolását kellett elvégezni. A minta adataiban 13 féle hibatipus fordult elő. Az anyagcsoport kódja pedig megmutatja, hogy pl. az 5-ös kód a fuvarelszámolási, a 6-os kód a bérelszámolási rendszerek csoportját jelenti. A mintában 15 féle anyagcsoporthoz tartoztak az adatok. A gyakoriság kód 1-5-ig terjedő értékeket kapott attól függően, hogy az anyag milyen időközökben kerül futtatásra. Pl. az egyes kód a napi, az ötös kód az évi egyszeri futás kódja.

Először az általános statisztikák kiszámitása történt meg. Az általános statisztikák irányt mutatnak a további vizsgálódáshoz. A statisztika azt mutatja, hogy időben nem egyenletes a hibák eloszlása. A hónapok között kétszeres különbségek vannak a hibás feldolgozások gyakoriságszámát figyelembevéve.

A hibáknak a kárnagyság szerinti eloszlását is kiszámitottam. A károsszeget az ujra futtatás időigényének a figyelembe vételével számitottam ki./Önkényesen feltételezve a monó üzemmódot és 2000,- Ft/gépóra dijat./

Megállapitható, hogy az esetek 53 %-ánál 500,- és 2.500,- Ft közé esett a hibakár értéke. A hibatipus szerinti elosztás a következő eredményt hozta.

Kiugróan magas volt a géphibák száma /több mint 50 %/ és közel azonos sullyal fordultak elő az operátori, futtatási, adatállomány vesztési hibák /8-10 %/. Vizsgálható az is, hogy a hibák hogyan oszlanak meg az anyagfelelősök szerint. Kiderült, hogy a hibák 65 %-a 3 anyagfelelős személyéhez kötődik, a többi 7-nek következésképpen csak a hibák 35 %-ával van kapcsolata. Az általános statisztikai jellemzők értékei azt mutatják, hogy az okozott kár 30 % 1.500,-, 50 % 2.000,- és 80 % 6.000,- Ft károsszeg értékhatár alá tartozik. Az átlagösszeg 3.868 Ft, a szórás pedig 4.555 Ft érték. A terjedelem felső határa 26.000,- Ft.

Azoknál a hibáknál, ahol külső kár is előfordul,a károsszeget különböző faktor értékekkel sulyozhatjuk, és a jellemzőket kiszámolhatjuk.

A fenti statisztikák alapján az elemzést két irányban folytattam tovább.

Az anyagfelelősök hiba-elosztását az időszak és a kárnagyság szerint elemeztem. Példaként egy anyagfelelős adatait mutatom be, azonban természetesen teljeskörüen kell ezt a vizsgálatot is elvégezni.

A 73-as kódu személynél a - december, az október és a junius a kritikus időszak a hibák 45 %-a fordul elő ezekben a hónapokban.
Érdekes eredményt mutat az egyes hibatipusok, a károsszeg szerinti eloszlása.

A 441 ezer Ft összhibából a gép 259 ezer, az operátori adatállomány tévedés 17 ezer, a futtatási hiba 45 ezer Ft-tal veszi ki részét.
Az elemzés igen fontos mozzanata az, amikor kisérletet teszünk arra vonatkozóan, hogy a hibatipusokat anyagcsoportok

szerint elemezzük. Kimondható-e az, hogy egy anyagcsoportba tartozó rendszerek hibái tipikusak, annak ellenére, hogy a rendszerek futtatási körülményei különbözőek, ill. ezeket a rendszereket más személyek készitették. Az elemzésbe csak azokat az anyagcsoportokat vontam be, ahol magas a rendszerhibák gyakorisága.

Megállapitható, hogy a 73-as kódu személy 10-es anyagcsoportba tartozó anyagánál összesen 22-szer hibázott, és a 10-es anyagcsoportba tartozó anyagoknál gyakran fordulnak elő az adatállományok téves kezelésével kapcsolatos esetek.

A vizsgálat továbbfolytatható különböző feltételek felállitásával. Pl. Van-e összefüggés a hibatipusok és a rendszerek ujrafuttatásának ideje között, vagy annak kimutatásával van-e összefüggés a hibatipusok és a rendszer készitésének időpontja között. Az egyes hibatipusok előfordulása esetén milyen szintü beavatkozásra van szükség az ujrafuttatás során.

Az elemzés módszere ismertetésének a végére értem. Tudom, szükségesnek látszik a módszer továbbfejlesztése, a feladathoz történő folyamatos módositása. Jelenleg előkészités alatt van egy teljes év rendszermeghibásodásainak feldolgozása. Az igy kapott eredmény birtokában a rendszertervezéshez és az üzemeltetéshez igen jelentős és megalapozott ajánlások tehetők.

Hangsulyozni szeretném, hogy minden esetben a helyi viszonyok feltárása alapján lehet csak konkrét, a munka minőségét javitó javaslatokat tenni.
Igy most összegzésemben óvatosan kerülöm az általánositásokat.

Ha figyelembe vesszük a minta-adatokat, a számitógépes rendszer, és a felhasználó kapcsolatában elgondolkoztató eredményt kapunk. Azt, hogy a felhasználó csak a legritkább esetben okozza a rendszer hibás müködését. A másik lényeges megállapitás, hogy szerencsére nem a bünözés, vagy az elemi csapások okozta kár jelnti a legfőbb gondot. Ezzel a véleményemmel nem az idevonatkozó előirások, és védelmi eszközök jogosságát kérdőjelezem meg, tisztában vagyok ezek fontosságával.

A mintavétel során előforduló hibatipusok azt mutatják, hogy az ellenőrzési eljárások nem épülnek be kellően a rendszerekbe. A személyi és géphibák relative későn kerülnek felszinre. A számitógépes rendszerek tervezői ritkán használják ki a folyamatba épitett programozható ellenőrzési lehetőségeket, annak ellenére, hogy ezek leirásával az irodalomban már találkozhatunk. Az un. egyszeri hibák előfordulása pl. egyes kártya-anyagok eldobozolása a manuális ellenőrzési tevékenységek kidolgozatlanságát mutatja. Az input adatok tartalmi ellenőrzésénél a teljesség ellenőrzés hiánya okozza sok esetben a legtöbb gondot. Az operátori futtatási hibák egyes előfordulásait is a rendszerek hiányosságai teszik lehetővé. Megitélésem szerint kevés azoknak a rendszereknek a száma, ahol a feldolgozások futtatása csak az előirt operátori beavatkozások szerint mehet végbe, és ezzel ellentétes minden futtatási kisérletet a rendszer visszautasit.

Végezetül annyit szeretnék még elmondani, a rendszer biztonságának növeléséhez szükség van arra, hogy a rendszerkészitők megismerjék ezeket az elemzéseket.

Tanulnunk kell az elkövetett hibákból.

Csak igy biztositható, hogy a számitógépes alkalmazások megfeleljenek a felhasználók által joggal elvárt igényeknek.

Belokosztovszki László - dr. Kiss István:

A NEMZETKÖZI ON-LINE SZOLGÁLTATÁSOK EGYES ADATVÉDELMI PROBLÉMÁI

A számitástechnikai adatvédelem kérdései szerves részét képezik a társadalom információellátási folyamata fejlődésének. Az információ feldolgozás az utóbbi évtizedekben számottevően változott. Mig néhány évvel ezelőtt azadathordozók csaknem kizárólag akták és kartotékok voltak, az adatok pedig főleg lokális jelleggel birtak, addig a számitógépes adatfeldolgozás minőségileg uj helyzetet teremtett. Lehetővé válik nagy adattömegek gyakorlatilag határozatlan időre való tárolása, az adatok különböző célokra való összakapcsolása, feldolgozása, megoldódott a központi adattárolás, valamint az adatok decentralizált be- és kivitele. Az egyre növekvő információmennyiség munkaerő és költségkimélő kezelése, a felhasználás sokrétüségével szemben támasztott követelmények, egyrészről indokolják a számitógépes adatfeldolgozás alkalmazását, másrészről azonban ez a minőségi változás veszélyeket rejt magában. Különösen élesen jelentkezik a személyhez füződő jogok megsértésének veszélye. Ha az információfeldolgozást a magánszférában csak a gazdaságossági megfontolások, a hatósági szférában pedig csupán az ügyintézés racionalizálása vezérli, ugy azok a személyek akikről az információ feldolgozásra kerülne, nemcsak előnyökhöz jutnának, hanem hátrányokat is szenvednének. Mindaddig, amig nem tudjuk ki rendelkezik rólunk információval, s nem tudjuk, hogy az illető személy /szerv/ milyen módon használja fel, s kinek adja tovább azokat, szembe kell nézni azzal a veszéllyel, hogy olyan kép alakul ki rólunk, amely nem egyezik tényleges életünkkel és amelyeket nem is befolyásolhatunk. Az állampolgár tudni akarja, hogy ki, milyen információt dolgoz fel róla, s ezeket mire használja. Felmerül az

adatvédelem gondolata. Az adatvédelem fontos feladata, hogy számitógépes feldolgozás esetén mutasson rá az embereket illető lehetséges veszélyekre, az információfeldolgozást szoritsa határok közé.
Az adatvédelemnek nyilvánvalóan nem az a célja, hogy megakadályozza a számitógépes adatfeldolgozás alkalmazását, hanem arról kell gondoskodnia, hogy a felhasználás ott végződjék, ahol a magánszféra kezdődik, ahol védelemre érdemes érdekeinket, az információk titokbantartásával kapcsolatban érvényre tudjuk juttatni. Itt kerül napvilágra az adatvédelem alapvető problémája: az emberek együttélésénél szükség van az információ továbbadására, de vajon hol van a határ a társadalom jóléte, az egyéni szabadság és az információhoz való hozzáférés elleni védelem között? A probléma távoli régiókba vezet.

Előadásunkban a számitástechnikai adatvédelem szerteágazó és komplex kérdései közül egy viszonylag szükebb területtel: az OMFB REI egyik tevékenységi körébe tartozó nemzetközi számitógépes on-line szolgáltatások koordinálásával összefüggő adatvédelmi problémákkal foglalkozunk.

Magyarországon először a nyugati közüzemi on-line számitógépes szolgáltatás megjelenése és bevezetése kezdeti feltételeinek megteremtésére az OMFB REI és az MTA SzTAKI között kialakult együttmüködés keretében került sor. A hálózati kapcsolatok müszaki kérdéseivel az MTA SzTAKI foglalkozott, a szolgáltatások szervezési, jogi, pénzügyi, biztonsági, propaganda tevékenységét az OMFB REI végezte.

Az MTA SzTAKI-ban folyó előrehaladott, és Magyarországon egyedülálló számitógépes hálózat-fejlesztési munkák nemzetközi hálózatokba történő bekapcsolódására a Nemzetközi Alkal-

mazott Rendszerelemzési Intézetben /IIASA, amelynek magyar bázisszervezete az OMFB REI/ folyó hasonló kutatások adtak módot. Az IIASA saját kutatási feltételeinek biztositására kapcsolatot épitett ki a Bécsi Müszaki Egyetem, az olaszországi CNUCE számitógéperőforrásaival, és igénybe vette az ESA, valamint a Tymnet-Telenet hálózaton keresztül elérhető nemzetközi számitóközpontok és adatbankok szolgáltatásait. Ezeket a szolgáltatásokat felajánlotta a tagországoknak is.

Ezt a IIASA nyujtotta lehetőséget elsőként a magyar tagszervezet ismerte fel, s az MTA SzTAKI-ban kinálkozó technikai feltételekre épitve - amelyek a hálózati kapcsolatok szükséges, de nem elégséges feltételeit biztositották - a szükséges szervezési lépéseket felmérve és elvégezve a szocialista országok közül elsőként valósitotta meg az összeköttetést, és alakitotta ki egy kisérleti üzemeltetés feltételeit. A kisérleti üzemeltetés 1982 elejéig tartott, majd a IIASA-tól különválva közüzemi szolgáltatásba ment át.

A szervezési munkákra 1978-79-ben került sor. Az IIASA-ban ekkor még nem álltak rendelkezésre a határátlépő információforgalom nemzetközi jogi, pénzügyi megállapodásai, ezért a szolgáltatást nyujtó külföldi intézményekkel külön-külön meg kellett állapodni a szolgáltatások használatának feltételeiről.

Az egyeztetések során a következő szempontokat vettük figyelembe:

- a számitógéperőforrásokhoz való hozzáférés hasznossága, politikai jelentősége,
- a kapcsolódás pénzügyi és adminisztrativ ellenőrizhetősége, a meglévő számitástechnikai védelmi szabályzatokra épülve,

- a kommunikáció iránya,
- a lekérdezett adatok jellege /személyhez füződő jogok kérdése/.

Ezek eredményeként a SzTAKI-val közösen kidolgoztuk a Nemzetközi Hálózati Végállomás Üzemeltetési Ügyrendjét. /Melléklet/

A kisérleti üzem során több mint 30 intézmény szakemberei végeztek rendszeres lekérdezéseket a legkülönbözőbb tudományos-müszaki, gazdasági témakörökből.

A témák nem érintettek személyvonatkozásu adatokat.

A számitástechnikai rendszerek titok-, vagyon-, és tüzvédelméről szóló 1/1981 /I.27./ BM. sz. rendelet végrehajtására az OMFB elnöke több társintézet elnökével közösen utasitást adtott ki. Ennek 6. §-a foglalkozott a nemzetközi távadatfeldolgozási és adattávközlési forgalommal. A korábban kialakitott NHV ügyrend megfelel az utasitás követelményeinek. Következetes naplózást végzünk. A gépnaplóba bevezetjük a következő adatokat: dátum, belépés kezdete, vége, felhasznált gépidő, munkavégző neve, intézete, adatvonal jellege, igénybevett hálózat, szolgáltatás, nyomtatott anyag oldalszáma, becsült költség, aláirás, megjegyzés.

A számitógépes információforgalomnak azonban vannak más veszélyei is. Annak ellenére, hogy jelenleg csak látszólag semleges lekérdezéseket végzünk, a kérdések jellegéből következtetni lehet arra, hogy ki mivel foglalkozik. Ez egyes kutatási területeken pl. gyógyszerkutatás, vegyészet, titkositási problémákat vet fel. A kérdésekből leszürhető következtetések levonását lehet zavarni, nehezíteni, azonban minden keresőnek magának kell megitélnie, hogy milyen költségvonza-

tu és ezzel összefüggő milyen mértékü zavarást érdemes alkalmaznia.

Másik fontos probléma az adatvédelem egy másik oldalát érinti, ez a világméretü információs küzdelem. A nemzetközi információforgalom során egyre inkább nyilvánvalóvá válik, hogy az információ uj hatalmi tényezőként jelenik meg. Birtoklása, termelése és elosztása feletti ellenőrzési jog része a politikai hatalomnak, sőt hatékony fegyverként is alkalmazható.

Példaként emlithető az USA Szovjetunióval szemben megnyilvánuló kemény vonala részeként az információáramlás korlátozása, /high technology/. A két világrendszer versenye már nem csak klasszikus pályákon, hanem információson is folyik.

A kelet-nyugati információcsere elősegitésére létrehozott intézményeket figyelmeztették, ne nyujtsanak segitséget a szocialista országoknak technikai fontosságu információ elérésében.

A szakmai folyóiratok rendszeres beszámolókat közölnek pl. a Tymnet-Telenet és az EURONET kiélezett versenyéről, és gyakran "információs háborut" emlegetnek, amely nem mindig irányul egyértelmüen a kelet ellen, szitja a nyugati világon belüli feszültségeket is. Az USA-nak az információ piacon való hegemóniai törekvései kedvezőtlen visszhangot váltanak ki a többi fejlett nyugati ország részéről is, mivel őket is kedvezőtlenül érinti az a tény, hogy az USA idegenkedik olyan információs file-k SzU részéről történő USA hálózaton keresztüli hozzáférésétől, mely adatbázisok származási helye többek között Nagy-Britannia, Benelux államok, Ausztria, Franciaország stb.

Az USA kormányzat nyilvánvaló intézkedései, melyek az információt törvényesitett politikai és taktikai fegyverként kezelik, jogosan váltja ki a többi ország ellenreakcióját, ami oda vezet, hogy USA-n kivül információs forrásokra épitenek ki csatornákat - akár más országok, akár saját adatbázisok kiépitése révén. Igy függetlenithetik magukat az USA adminisztráció kénye-kedvétől, ami számukra kedvezőtlen esetben, olyan paradoxon helyzethez vezethet, hogy saját országukból származó USA-hálózaton elérhető adatokat nem érhetnének el. Ez végül is szüklátókörü, önellátó információtermeléshez vezetne.

Ha elfogadjuk a szabad információáramlás /géppel olvasható információ/ elvét, akkor az információt minden feltételtől függetlenül, elválasztva a fegyverektől, stratégiai cikkektől, szabadon hozzáférhetővé kell tenni, haszonlóan a nyomtatott könyvekéhez és egyéb sajtótermékhez.

A kérdés azonban tulmutat a számitógépes adatvédelem kérdésén, és egy széleskörü, egységes információpolitika kidolgozását igényli.